COMTREND CORPORATION

NexusLink 5631E

Wireless ADSL2+ Bonded Router for Annex B

User's Manual

Version C2.0, February 1, 2008

261076-004

Warning

- Before servicing or disassembling this equipment, always disconnect all power and telephone lines from the router.
- Use an appropriate power supply and a UL Listed telephone line cord. Specification of the power supply is clearly stated in Appendix E.

Preface

This manual provides information for network administrators. It covers the installation, operation and applications of this router. The individual reading this manual is presumed to have a basic understanding of telecommunications.

This document is subject to change without notice. For product updates, new product releases, manual revisions, software upgrades, etc., visit our website at http://www.comtrend.com

Copyright

Copyright© 2007 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without the prior written consent of Comtrend Corporation.

Technical support

If you find the product to be inoperable or malfunctioning, please contact a technical support engineer for immediate service by email at INT-support@comtrend.com

Save Our Environment

This symbol means that when the equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this router can be recycled in accordance with regionally established regulations.

Never throw-out this electronic equipment along with your household waste. You may be subject to penalties or sanctions under the law. Instead, ask for instructions from your municipal government on how to correctly dispose of it. Please be responsible and protect our environment.

Table of Contents

Chapter 1 Introduction

The NexusLink 5631E Wireless ADSL2+ Bonded Router for Annex B features flexible networking connectivity with dual ADSL line capability, four 10/100 Ethernet ports, two USB ports and an 802.11g wireless LAN access point. It has robust routing capabilities to segment and direct data streams and allows for multiple data encapsulations.

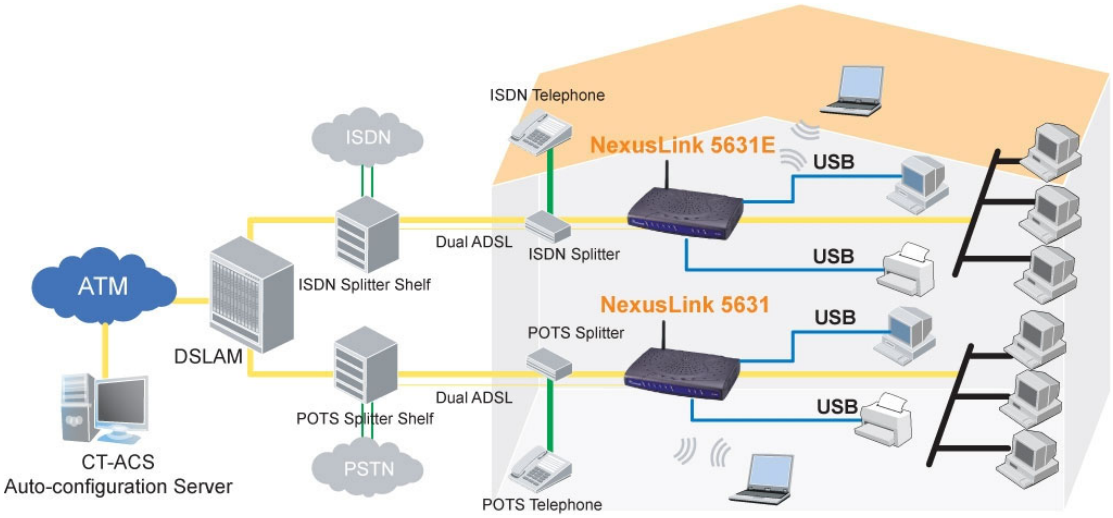
The NexusLink 5631E is a black box solution for deploying Triple Play architectures, doubling bandwidth (48Mbps) performance over traditional ADSL2+ modems. It provides higher level performance with embedded security, QoS, VPN and remote management functions. As an added bonus, the USB host acts as a printer hub and will enable future product enhancements available by software upgrade.

1.1 Features

- Dual ADSL2+ bonded
- Annex B (ISDN)
- UPnP installation
- Integrated 802.11g AP (WiFi)
- WPA and 802.1x
- RADIUS client
- IP /MAC address filtering
- Static route/RIP/RIP v2 routing functions
- Dynamic IP assignment
- NAT/PAT
- IGMP Proxy and fast leave
- DHCP Server/Relay/Client
- DNS Relay
- Auto PVC configuration
- Supports 16 VCs
- Embedded SNMP agent
- Web-based management
- Remote configuration and upgrade
- Supports TR-069/TR-098/TR-111 For Remote Management
- Configuration backup and restoration
- FTP server
- TFTP server

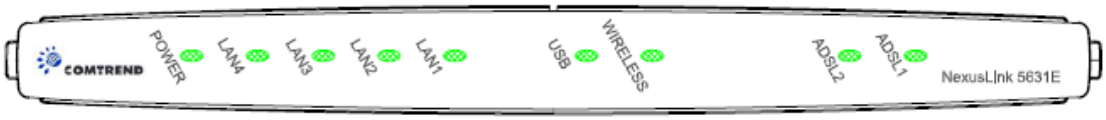
1.2 Application

This diagram depicts the application of the NexusLink 5631E on an ISDN connection. It also shows our related product NexusLink 5631 which is an Annex A device.



1.3 Front Panel LED Indicators

The front panel LED indicators are shown and explained below.

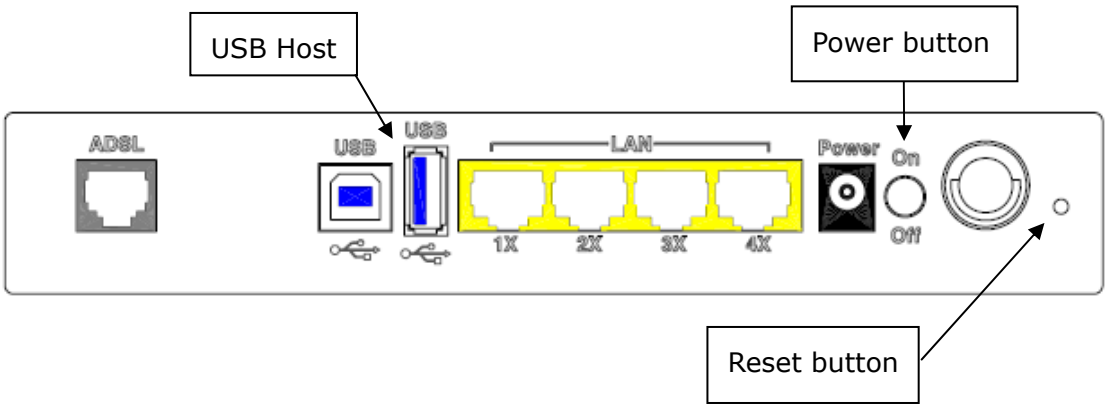


LED	Color	Mode	Function
POWER	Green	On	The router is powered up.
		Off	The router is powered down.
LAN 1~4	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
	Green	Blink	Data transmitting or receiving over LAN.
USB	Green	On	A USB link is established.
		Off	A USB link is not established.
	Green	Blink	Data transmitting or receiving over USB.
WIRELESS	Green	On	The Wireless is ready and idle.
		Off	The Wireless is not installed.
	Green	Blink	Data transmitting or receiving over Wireless
ADSL 1~2	Green	On	The ADSL link is established.
		Off	The ADSL link is not established.

Chapter 2 Installation

2.1 Hardware Installation

Follow the instructions below to complete the hardware installation.
A diagram of the back panel of the router is shown below for reference.



Connection to Power

Connect the power jack to the shipped power cord. Attach the power adapter to the wall outlet or other AC source. After all connections have been made, press the power button to turn on the router. After powering on, the router will perform a self-test. Wait a few moments and the router will be ready to operate.

Caution 1: If the router fails to power up, or if it malfunctions, first verify that the power supply is connected correctly. Then power it on again. If the problem persists, contact our technical support engineers.
Caution 2: Before servicing or disassembling this equipment always disconnect all power cords and telephone lines from the wall outlet.

Reset Button

In the rear panel, there is a reset button. To load the factory default settings, hold the reset button down for 5 to 10 seconds.

Connection to USB port

Connect the USB port to a PC with a standard USB cable.

Connection to USB host port

This router is equipped with one high-speed USB 2.0 host connection.
With software support, users can connect USB devices such as printers or a hard disc to the router. For this software release, only printer service is supported.

Connection to LAN port

To connect to a hub or PC, use a RJ45 cable. You can connect the router to four LAN devices. The ports are auto-sensing MDI/X and either straight-through cable or crossover cable can be used.

Connection to LINE port

If you wish to connect both the router and a telephone, connect the LINE port to a POTS splitter with a RJ14 cable.

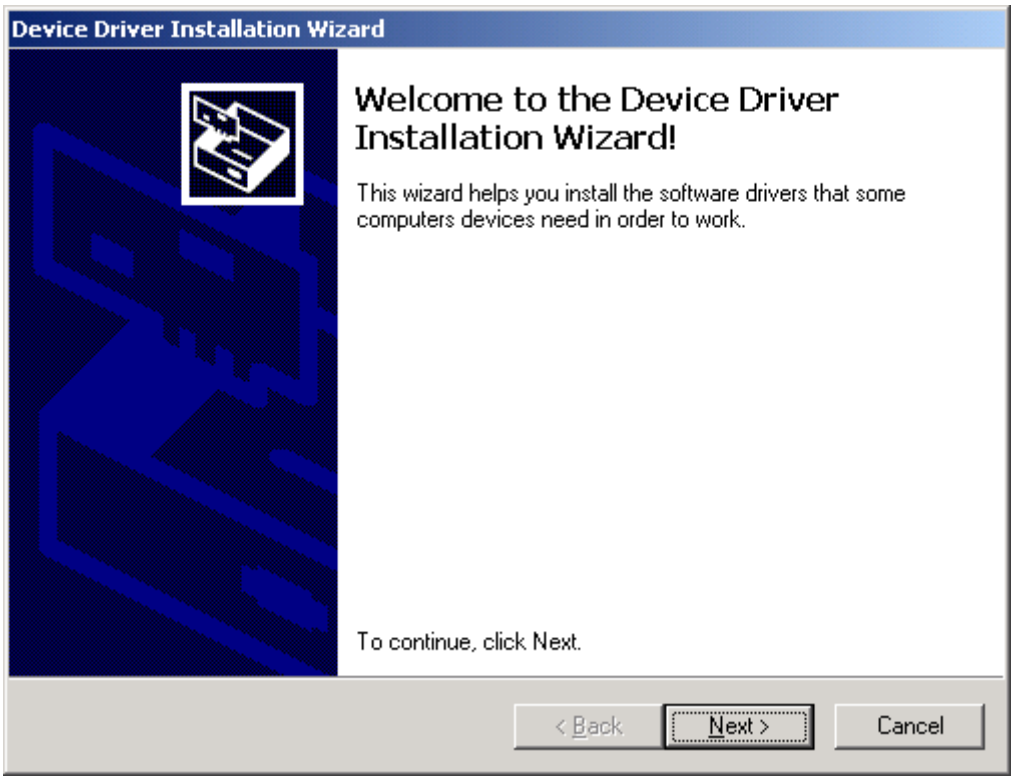
2.2 USB Driver Autorun Installation

Before connecting the router to a PC with USB, the correct drivers must be installed. The auto-run USB driver installation supports Win ME, Win 98, Win 2000, Win XP (32 bit) and Vista (32 bit). For those using Windows XP 64 bit, the driver must be installed manually (please see section 2.3 below for details).

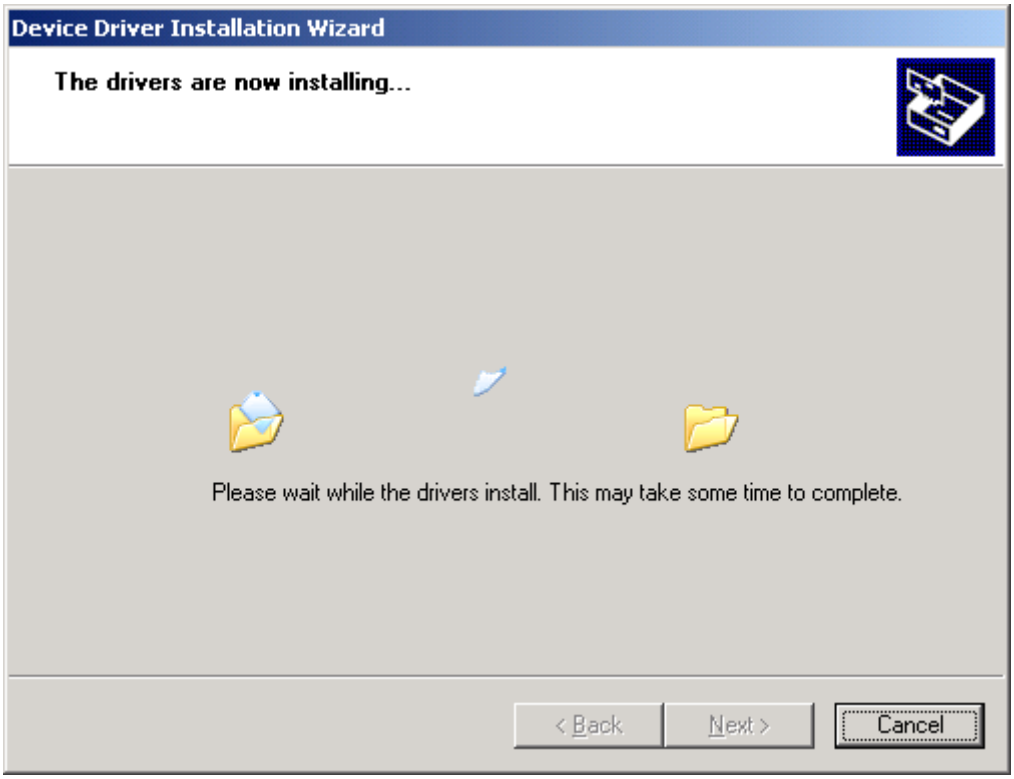
Follow the procedure below to install the standard (32 bit) USB driver

STEP 1: Insert the Installation CD and select **Install USB Driver** from the autostart menu options shown below.

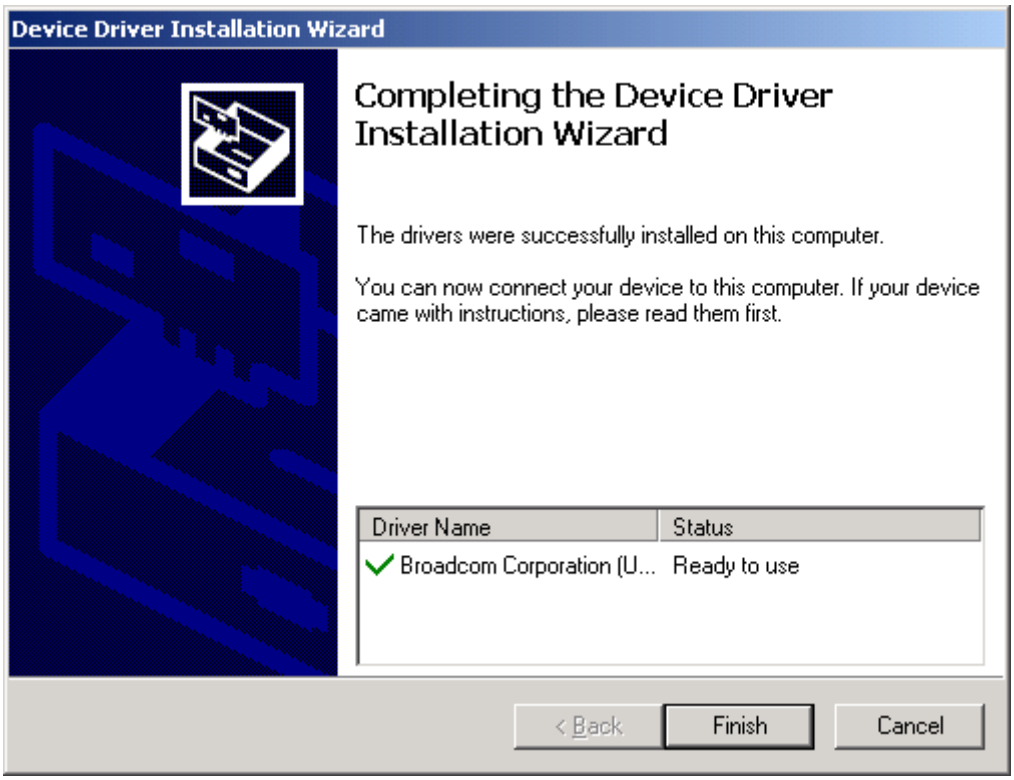
STEP 2: The following window will be displayed. Click the **Next** button to continue.



STEP 3: When the window displays as below, wait for the drivers to fully install.



STEP 4: Click the **Finish** button, when the window displays as below.



STEP 5: The installation is complete. You can now connect the router to your PC using a standard USB cable.

2.3 USB Driver Manual Installation (64bit OS)

Before connecting this router to a PC with USB, the correct drivers must be installed.

Follow the procedure below to manually install the 64bit USB driver

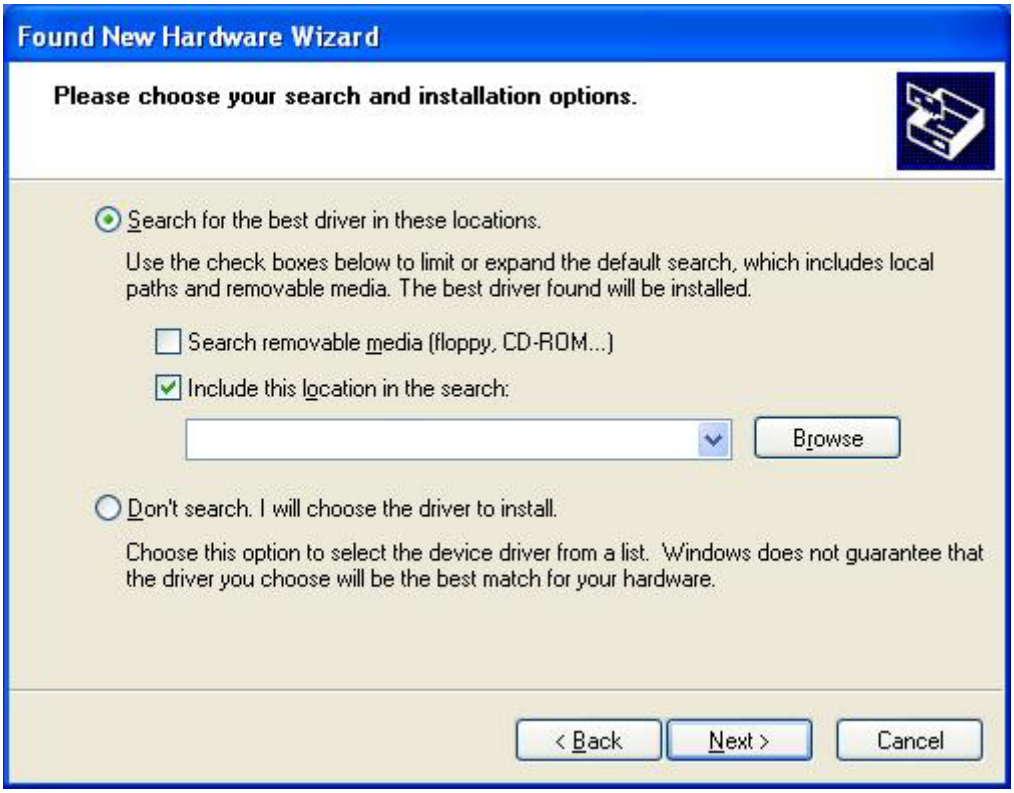
STEP 1: Connect the USB port to the PC by plugging the flat connector of a standard USB cable into your PC and plugging the square connector into the router. After a moment, your router should be detected by your PC and if so the screen will display a notice to that effect, as shown below:

STEP 2: When the window displays as below, select **Install from a list or specific location (Advanced)** and then click the **Next** button.

Note:	This window won't display if the USB Driver has been previously installed. In this case, contact technical support for assistance.

STEP 3: Insert the installation CD.

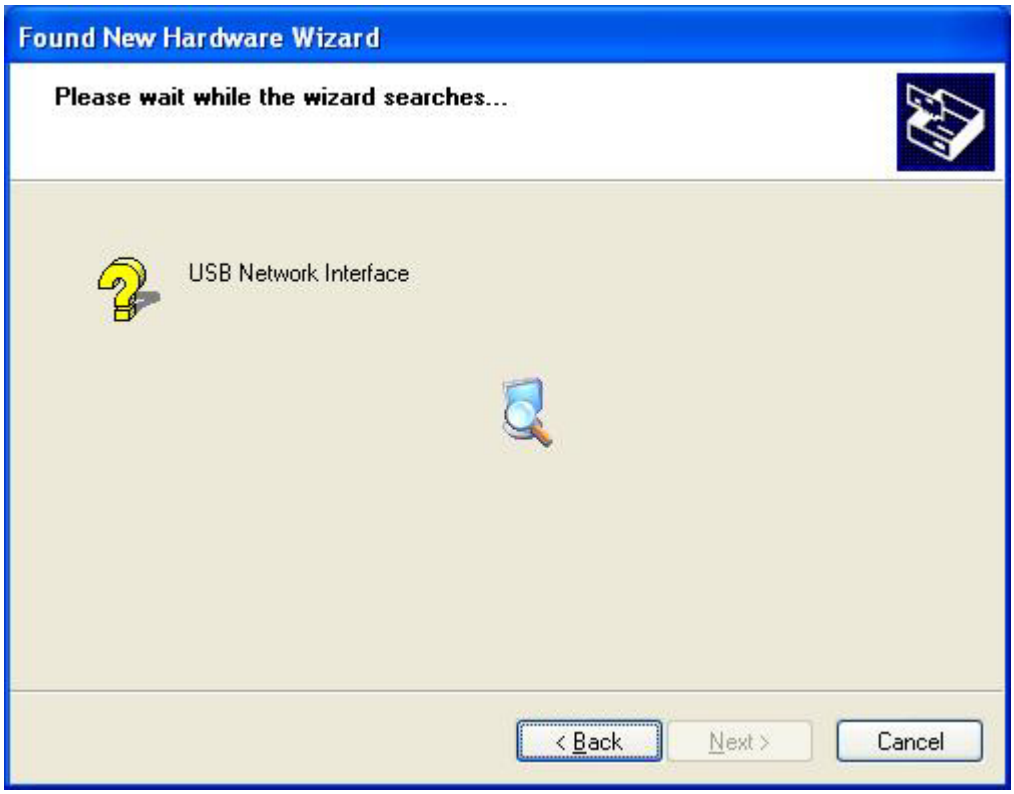
Note:	If you see the autostart menu (as shown in **step 1** of previous section) **CLICK -**  and continue with the manual installation process.

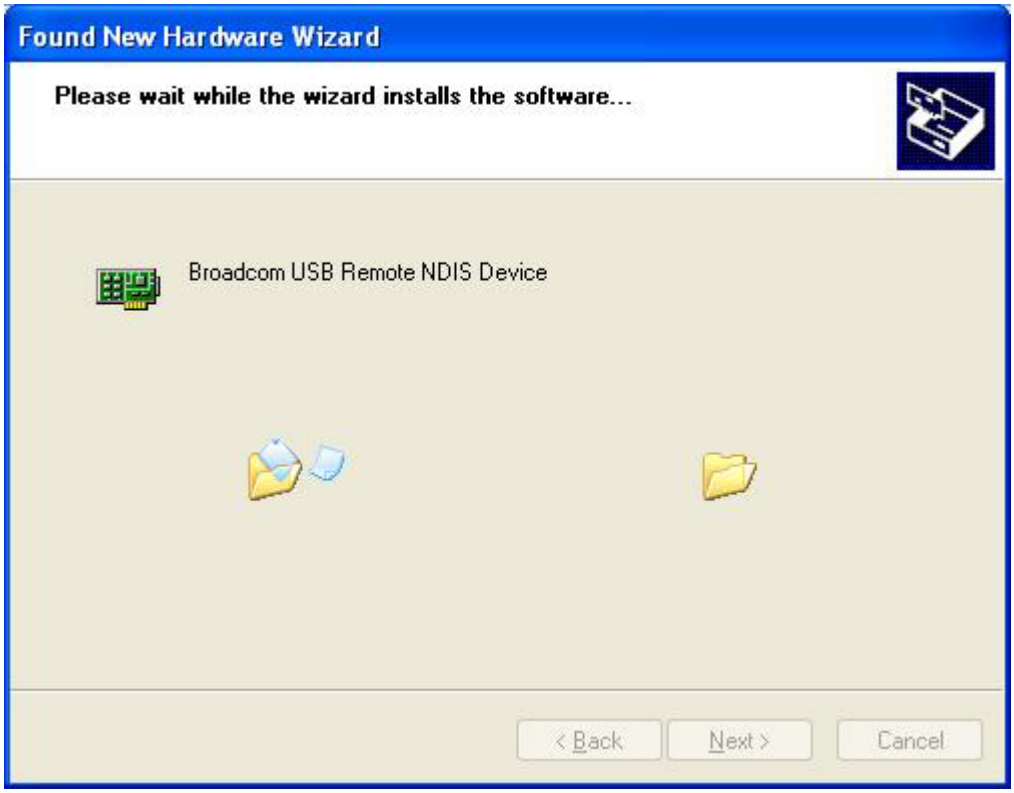


STEP 4: Select the location of the file using the **Browse** button, as shown above. Normally, the file is on the CD-ROM shipped with the router.

STEP 5: Locate the **Vista** folder, and click **OK**.

STEP 6: When the window displays as below, click the **NEXT** button and wait.





STEP 7: Click the **Finish** button when the window displays as below.

STEP 8: Installation is complete.

Chapter 3 Web User Interface

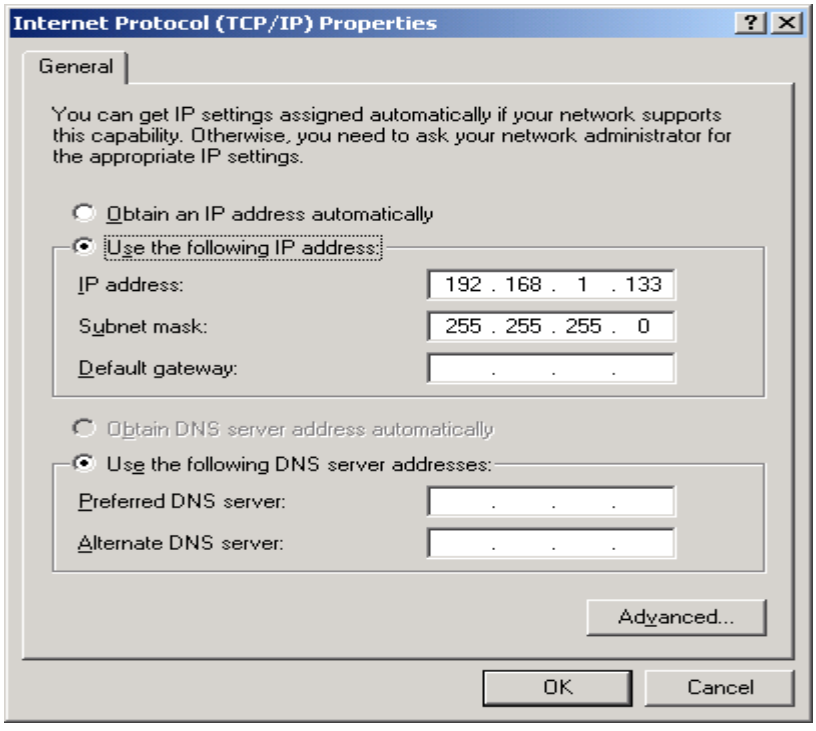
This section describes how to manage the router via a web browser. The web page is best viewed with Microsoft Internet Explorer 5.0 and later. A unique default user account is assigned with user name **root** and password **12345**. The user can change the default password later when logged in to the router.

3.1 TCP/IP Settings

The default IP address of the router (LAN port) is 192.168.1.1. To configure the router for the first time, the configuration PC must have a static IP address within the 192.168.1.x subnet. Follow the steps below to configure your PC IP address to use subnet 192.168.1.x.

STEP 1: Right click on the Local Area Connection under the Network and Dial-Up connection window and select **Properties**.

STEP 2: Enter the TCP/IP window and change the IP address to **192.168.1.x/24**.



STEP 3: Click OK to submit settings.

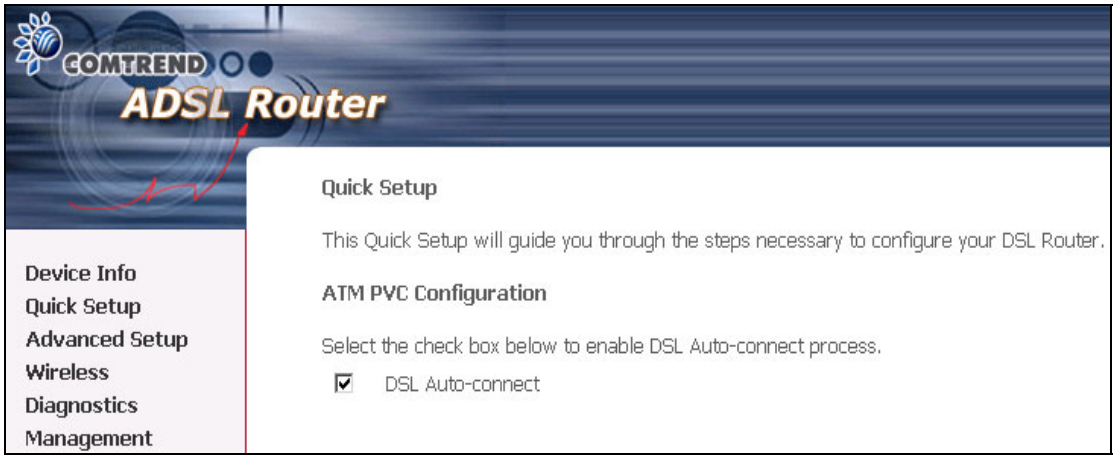
3.2 Login Procedure

Perform the following steps to bring up the web browser and configure the router.

STEP 1: Start the Internet browser. Type the IP address for the router in the Web address field. For example, if the IP address is 192.168.1.1, type http://192.168.1.1

STEP 2: You will be prompted to enter your user name and password. Type root for the user name and **12345** as the password, then click **OK**. These values can be changed later (see **section 9.6.3**).

STEP 3: After successfully logging in, you will reach the Quick Setup menu.



3.3 Default Settings

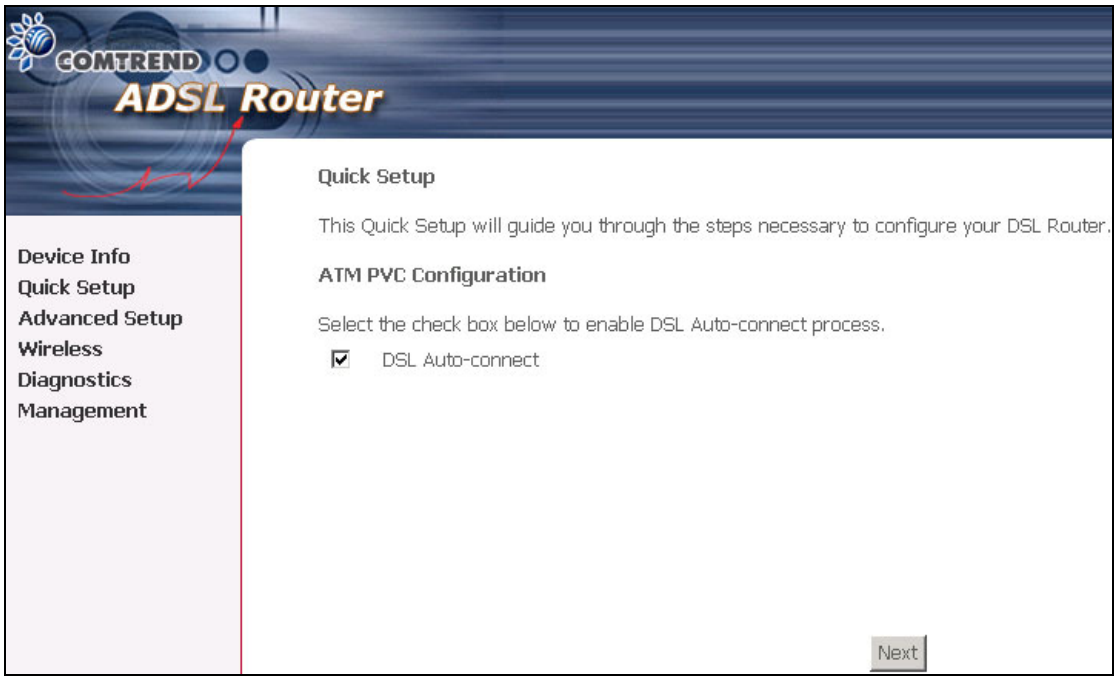
During power on initialization, the router sets all configuration attributes to default values. It will then read the configuration profile from flash memory. The default attributes are overwritten when identical attributes with different values are configured. The configuration profile can be created via the web browser, telnet user interface or other management protocols. The factory default configuration can be restored either by resetting the router or by clicking the Restore Default Configuration option in the Restore Settings screen (see **section 9.1.3**).

The following list shows the factory default settings for this router.

- LAN port IP address(es): 192.168.1.1 (ADSL1) and 192.168.1.2 (ADSL2)
- Local administrator account name: root
- Local administrator account password: 12345
- Local non-administrator account name: user
- Local non-administrator account password: user
- Remote WAN access: disabled
- Remote WAN access account name: support
- Remote WAN access account password: support
- NAT and firewall: Disabled for MER, IPoA and Bridge modes
  Enabled for PPPoE and PPPoA modes
- DHCP server on LAN interface: enabled
- WAN IP address: none
- Wireless access: enabled
- SSID: Comtrend
- Wireless authentication: open (no authentication)
- Annex B enabled / Annex M disabled

Chapter 4 Quick Setup

After login, the **Quick Setup** screen will appear as shown.



NOTE:	The selections available on the main menu are based upon the configured connection and user account privileges.

The Quick Setup screen allows the user to configure the router for ADSL connectivity and Internet access. It also guides the user though the WAN network setup first and then the LAN interface setup. You can either manually customize the router or follow the online instruction to set up the router.

This router supports the following data encapsulation methods.

- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoA)
- MAC Encapsulated Routing (MER)
- IP over ATM (IPoA)
- Bridging

The following configuration considerations apply:

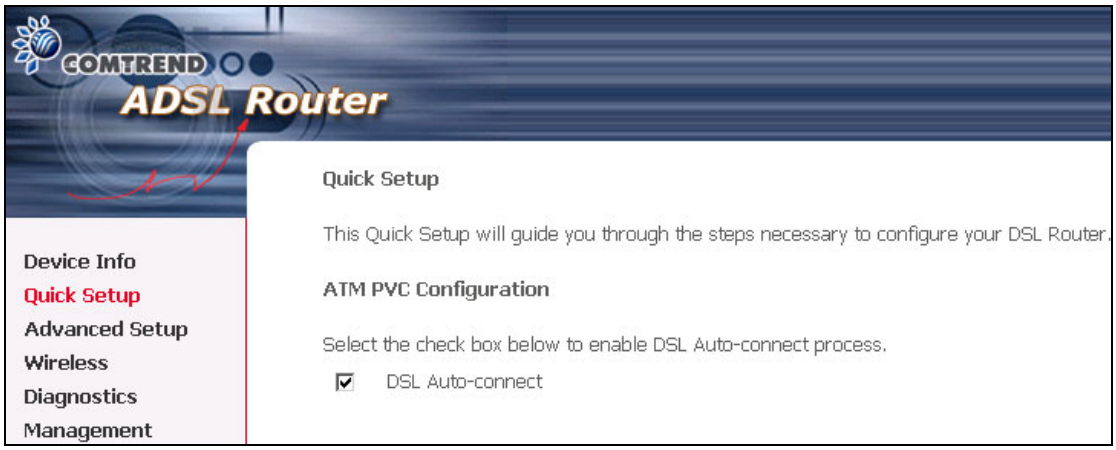
- The WAN network operating mode operation depends on the service provider's configuration in the Central Office and Broadband Access Server for the PVC
- If the service provider provides PPPoE service, then the connection selection depends on whether the LAN-side device (typically a PC) is running a PPPoE client or whether the router is to run the PPPoE client. The router can support both cases simultaneously.
- If some or none of the LAN-side devices do not run PPPoE client, then select PPPoE. If every LAN-side device is running a PPPoE client, then select Bridge In PPPoE mode, the router also supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices. In most cases, NAT and firewall should always be enabled when PPPoE or PPPoA mode are selected, but they can be enabled or disabled by the user when MER or IPoA is selected, NAT and firewall are always disabled when Bridge mode is selected.
- Depending on the network operating mode, and whether NAPT and firewall are enabled or disabled, the main panel will display or hide the NAPT/Firewall menu. For instance, at initial setup, the default network operating mode is Bridge. The main panel will not show the NAPT and Firewall menu.

NOTE:	Up to sixteen PVC profiles can be configured and saved on the flash memory. To activate a particular PVC profile, you need to navigate all the Quick Setup pages until the last summary page, then click on the Finish button and reboot the system.

4.1 Auto Quick Setup

The auto quick setup requires the ADSL link to be up. The ADSL router will automatically detect the PVC. You only need to follow the online instructions that you are prompted.

STEP 1: Select **Quick Setup** to display the Quick Setup screen.

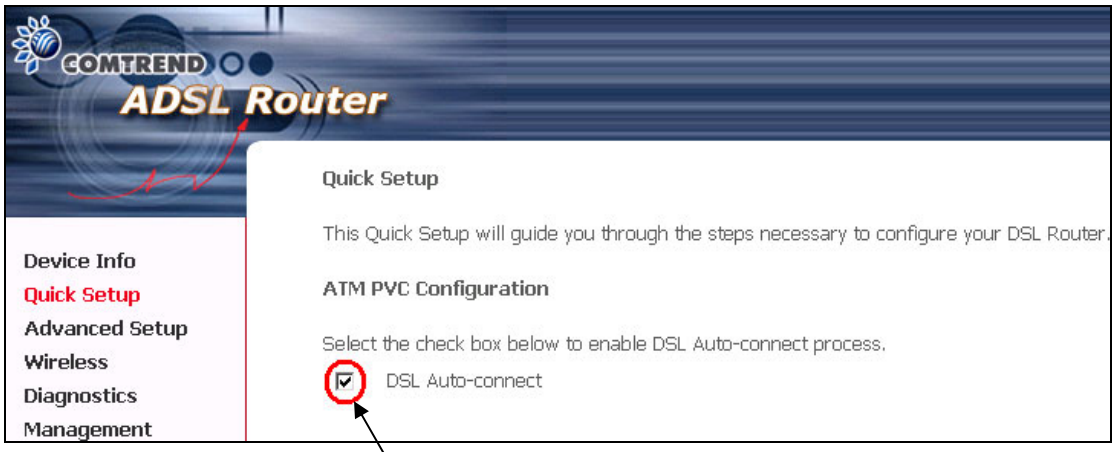


STEP 2: Click **Next** to start the setup process. Follow the online instructions to complete the setting. This procedure will skip some processes like PVC index, or encapsulation.

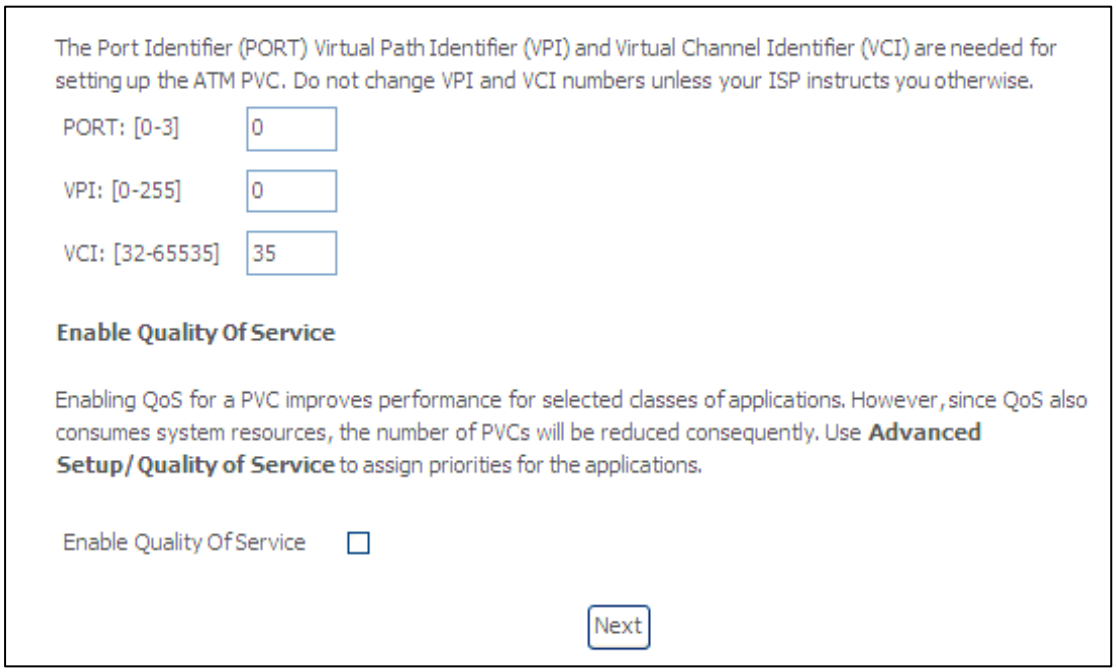
STEP 3: After the settings are complete, you can use the ADSL service.

4.2 Manual Quick Setup

STEP 1: Click **Quick Setup** and un-tick the **DSL Auto-connect** checkbox to enable manual configuration of the connection type.



Untick this checkbox to enable manual setup and display the following screen.

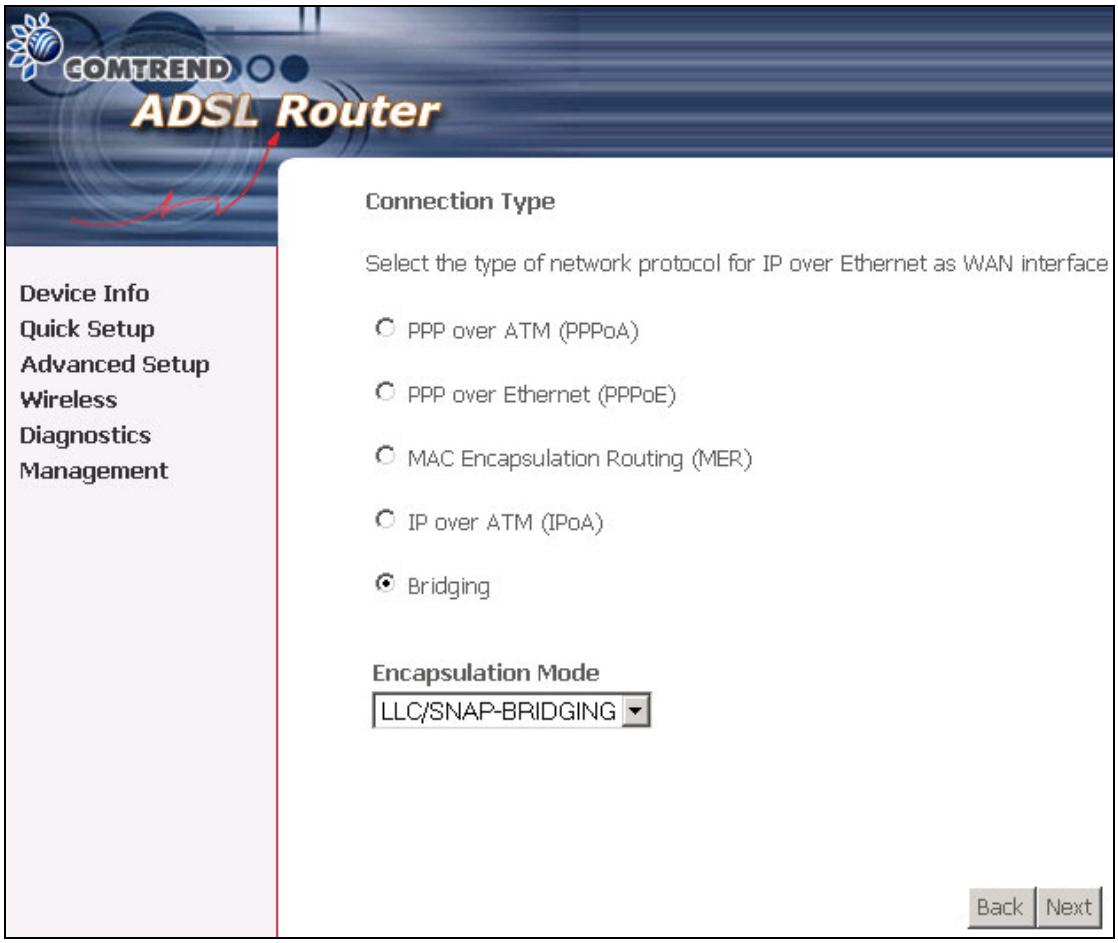


STEP 2: Enter the PORT, Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) values. Select Enable Quality Of Service if required and click **Next**.

STEP 3: Choose an Encapsulation mode.

Choosing different connection types provides different encapsulation modes.

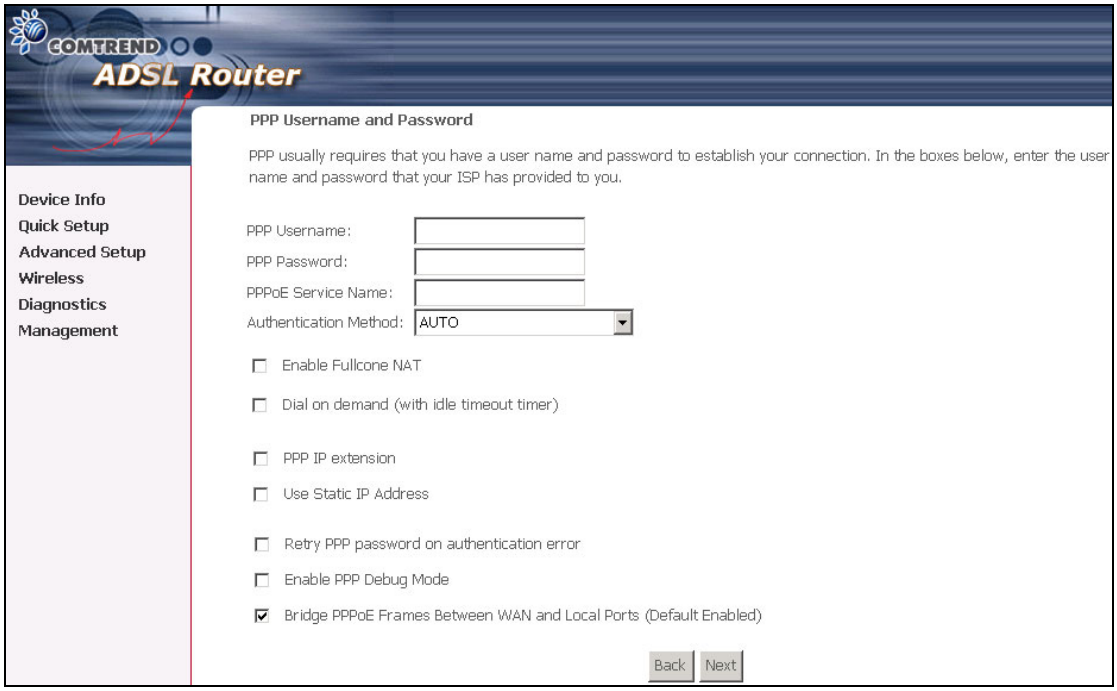
- PPPoA- VC/MUX, LLC/ENCAPSULATION
- PPPoE- LLC/SNAP BRIDGING, VC/MUX
- MER- LLC/SNAP-BRIDGING, VC/MUX
- IPoA- LLC/SNAP-ROUTING, VC MUX
- Bridging- LLC/SNAP-BRIDGING, VC/MUX



NOTE:	Subsections 4.2.1 - 4.2.4 describe the PVC setup procedure further. Choosing different connection types pops up different settings requests. Enter appropriate settings that are required by your service provider.

4.2.1 PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE)

STEP 4: Select the PPP over ATM (PPPoA) or PPP over Ethernet (PPPoE) radio button and click **Next**. The following screen appears.



Enable Fullcone NAT

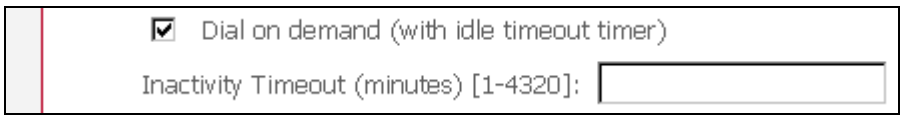
Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

PPP Username/PPP Password

The PPP Username and the PPP password requirement are dependent on the particular requirements of the ISP or the ADSL service provider. The WEB user interface allows a maximum of 256 characters in the PPP user name and a maximum of 32 characters in PPP password.

Disconnect if no activity

The router can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** check box. When the checkbox is ticked, you need to enter the inactivity timeout period. The timeout period ranges from 1 minute to 4320 minutes.



PPP IP Extension

The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specially requires this setup, do not select it.

The PPP IP Extension supports the following conditions:

- Allows only one PC on the LAN
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the ADSL router has a single IP address to assign to a LAN device.
- NAPT and firewall are disabled when this option is selected.
- The ADSL router becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The ADSL router extends the IP subnet at the remote service provider to the LAN PC. That is, the PC becomes a host belonging to the same IP subnet.
- The ADSL router bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the router's LAN IP address.

Use Static IP Address

Unless your service provider specially requires this setup, do not select it.

If selected, enter your static IP address.

Retry PPP password on authentication error

Tick the box to select.

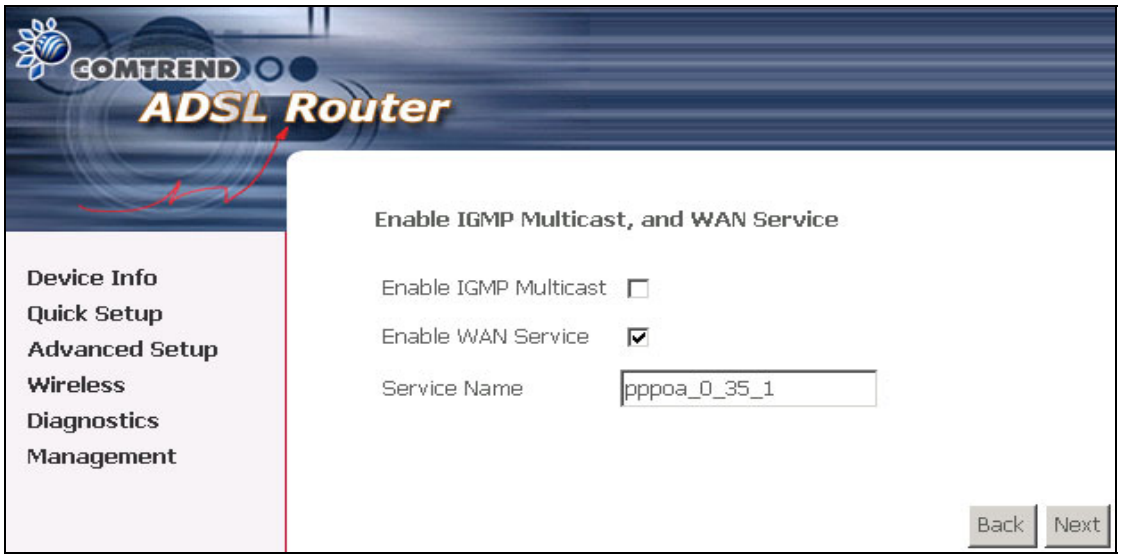
Enable PPP Debug Mode

Enable the PPPoE debug mode. The system will put more PPP connection information in System Log. But this is for debug, please don't enable in normal usage.

Bridge PPPoE Frames Between WAN and Local Ports (Default Enabled)

If Enabled, the function can create a local PPPoE connection to the WAN side.

STEP 5: Click **Next** to display the following screen.



Enable IGMP Multicast checkbox:

Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

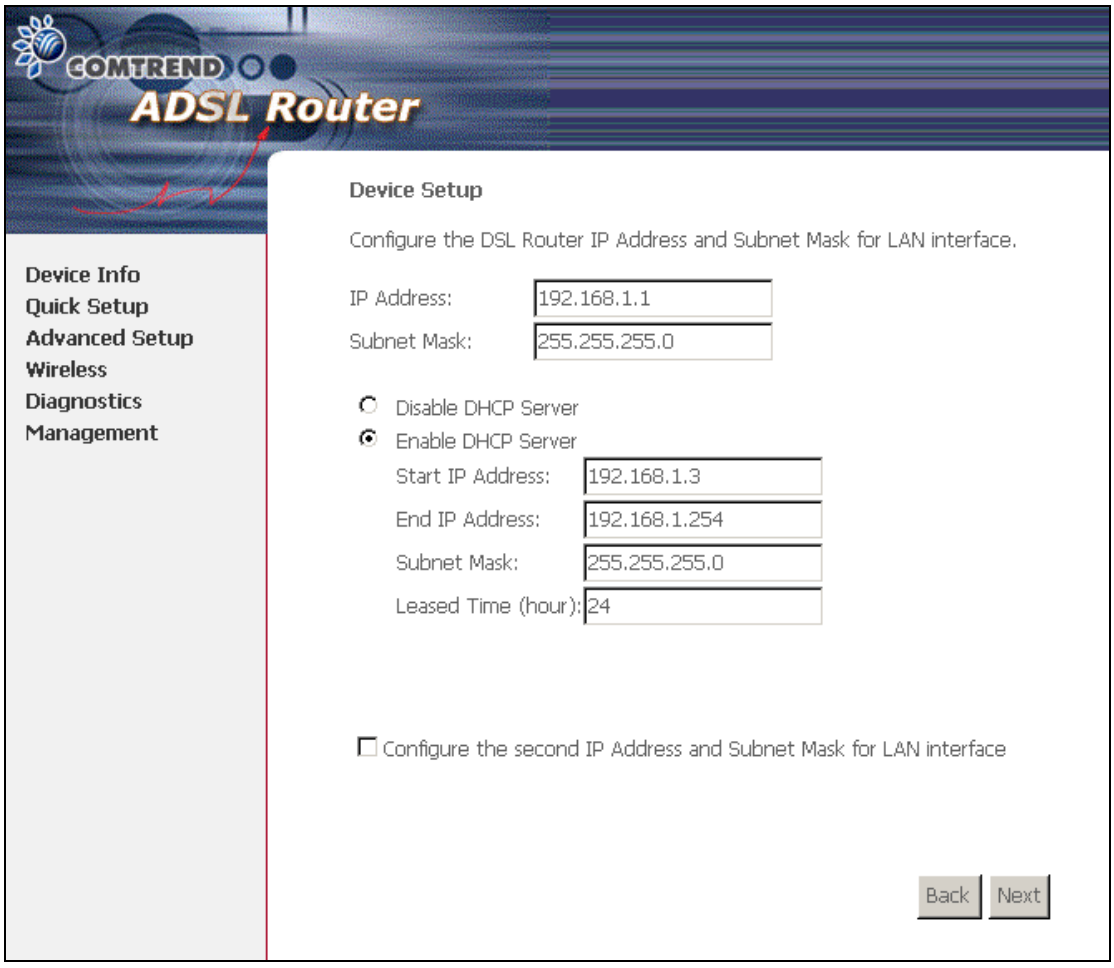
Enable WAN Service checkbox:

Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name:

This is user-defined.

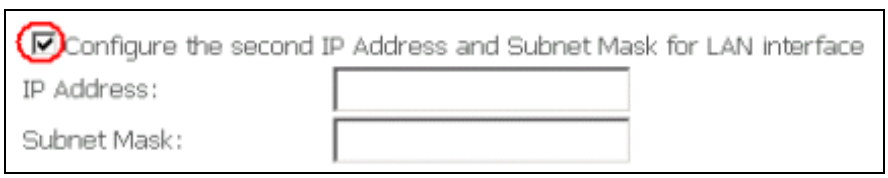
STEP 6: After entering your settings, select **Next**. The following screen appears.



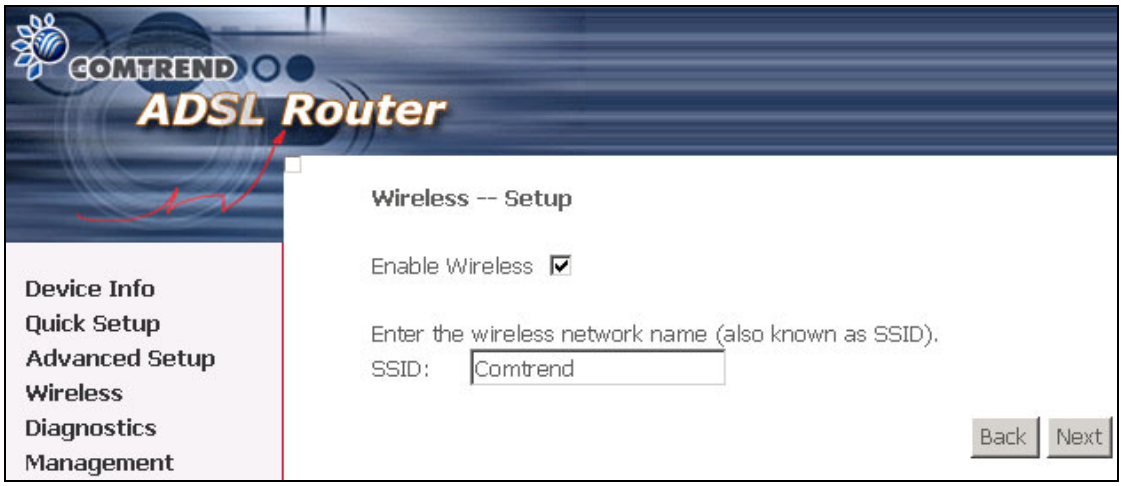
This page allows the user to configure the LAN interface IP address, subnet mask and DHCP server. If the user would like this ADSL router to assign dynamic IP address, DNS server and default gateways to other LAN devices, select the button **Enable DHCP server on the LAN** to enter the starting IP address and end IP address and DHCP leased time.

The Device Setup page allows the user to configure the LAN interface IP address and DHCP server. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

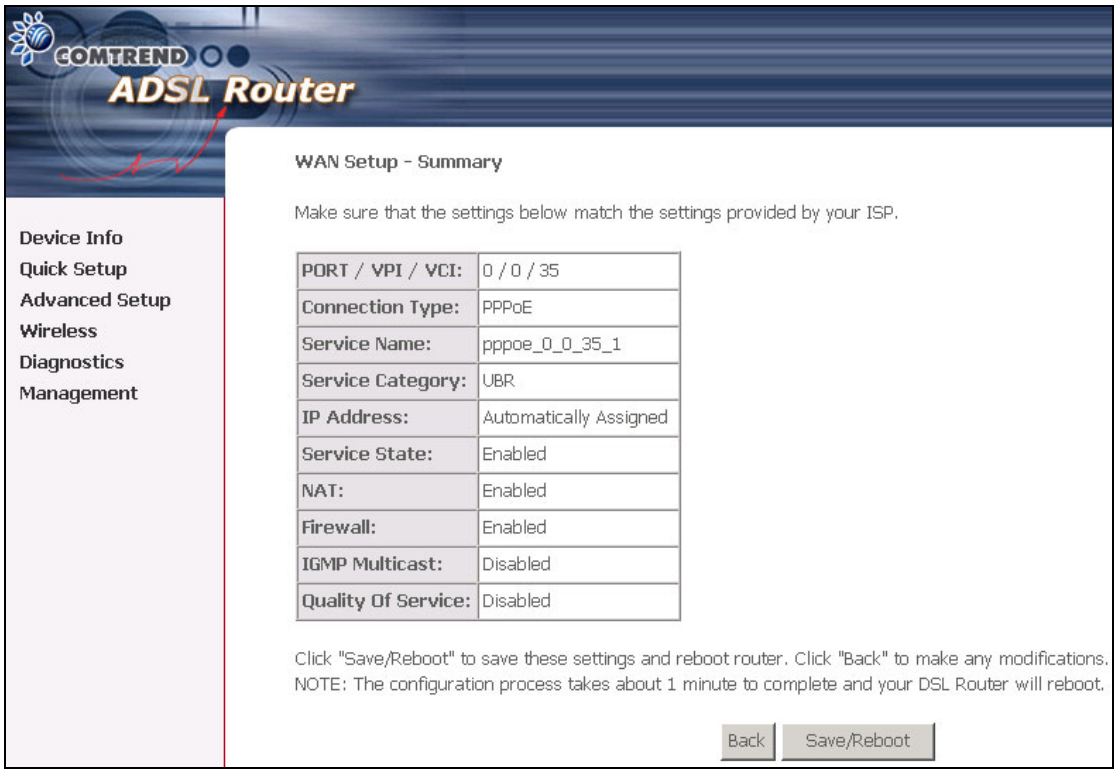
To configure a secondary IP address for the LAN port, click the box as shown below.



STEP 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown), input a new SSID (if desired) and click **Next**.



STEP 8: Click **Next** to display the WAN Setup-Summary screen that presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.

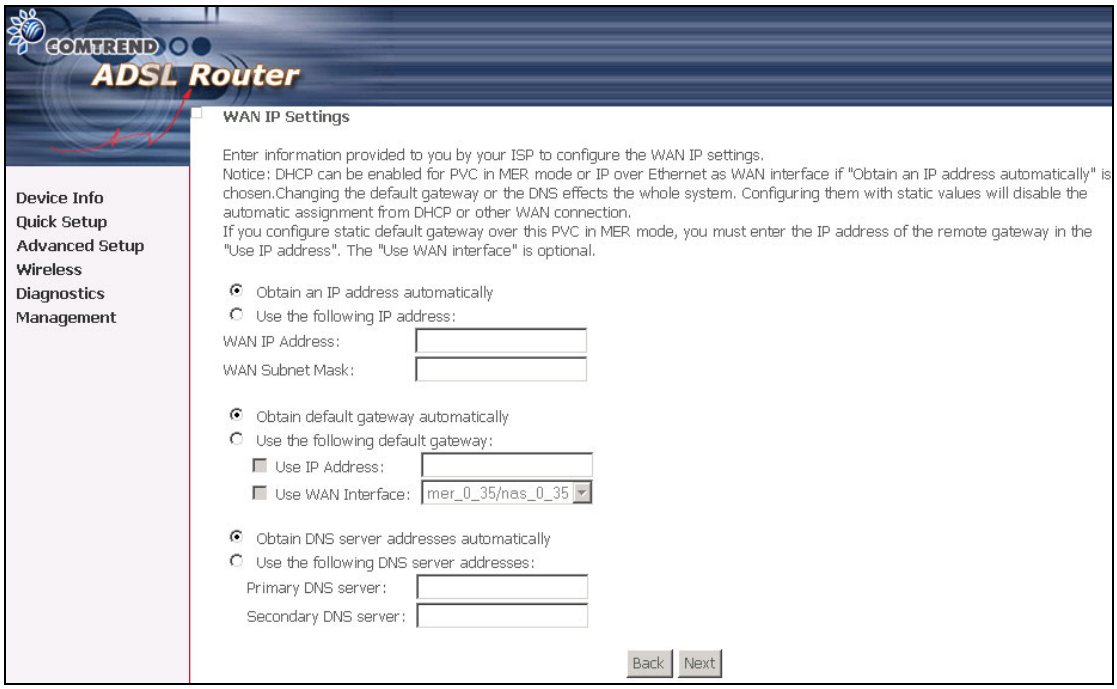


STEP 9: After clicking **Save/Reboot**, the router will save the configuration to flash memory and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info page automatically. The router is ready for operation when the LED indicators display as described in Chapter 1.3.

4.2.2 MAC Encapsulation Routing (MER)

Step 4: Select the MAC Encapsulation Routing (MER) radio button and click **Next**.

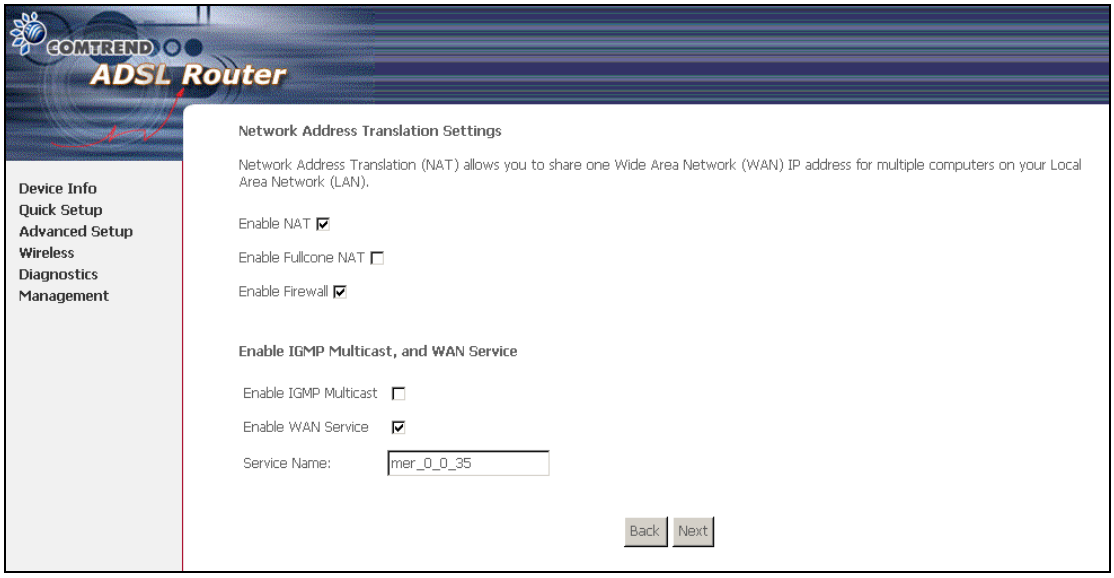
The following screen appears.



Enter information provided to you by your ISP to configure the WAN IP settings.

NOTE:	DHCP can be enabled for PVC in MER mode if **Obtain an IP address automatically** is chosen. Changing the default gateway or the DNS affects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection. If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address" field. The ISP will provide the values to enter in these fields.

Step 5: Click **Next** to display the following screen.



Enable NAT checkbox: If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu on the left side main panel will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side, this checkbox should be de-selected to free up system resources for better performance. When the system comes back after reboot, the NAT submenu will not be displayed on the left main panel.

Enable Fullcone NAT: This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

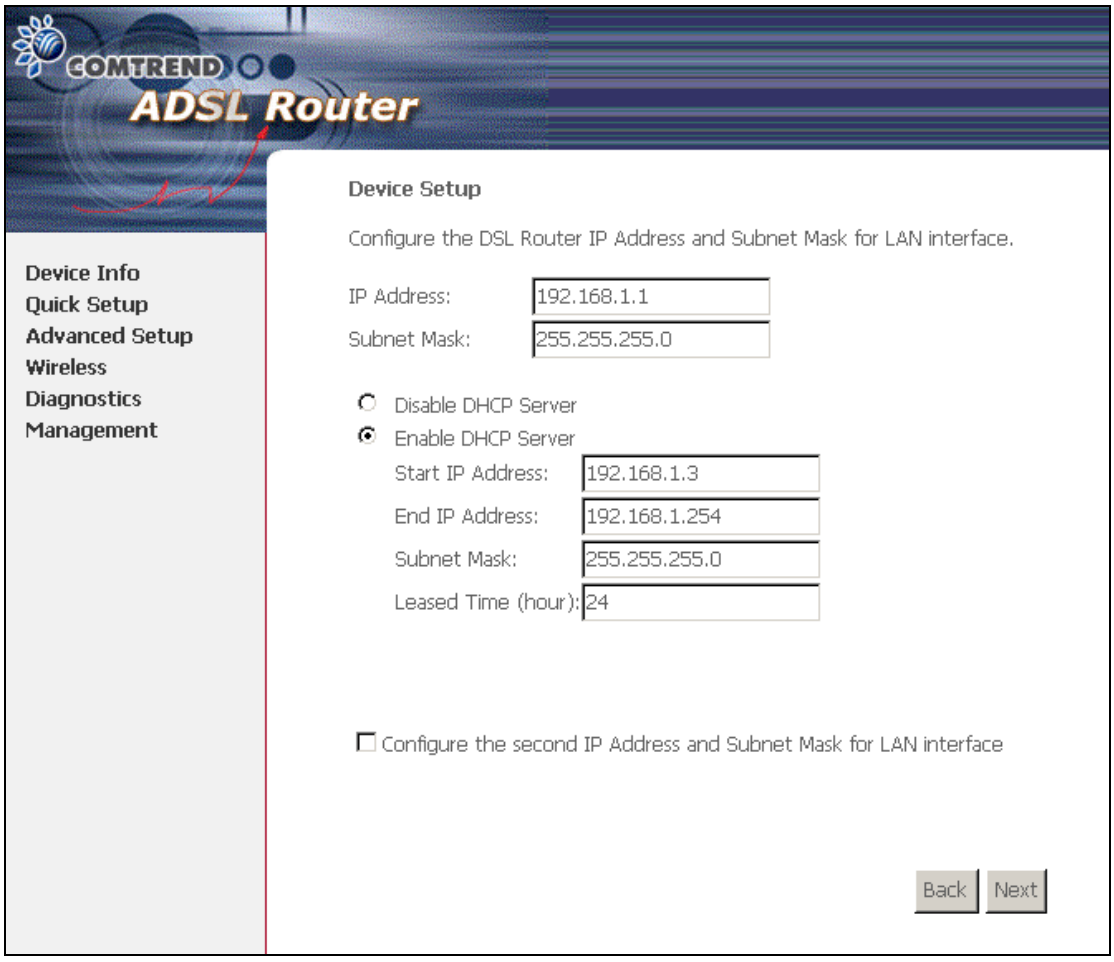
Enable Firewall checkbox: If the firewall checkbox is selected, the Security submenu on the left side main panel will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Security submenu will not be displayed on the left main panel.

Enable IGMP Multicast: Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

Enable WAN Service: Tick the checkbox to enable the WAN service. If this item is not selected, you will not be able to use the WAN service.

Service Name: This is User-defined.

Step 6: Upon completion click **Next**. The following screen appears.



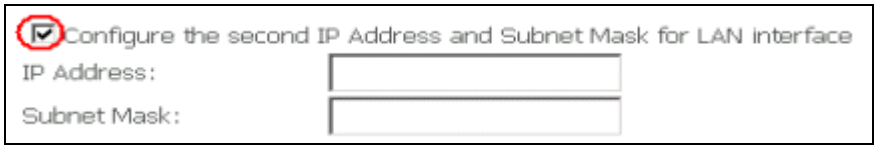
Consult the following paragraphs for more details about these settings.

The Device Setup page allows the user to configure the LAN interface IP address and DHCP server. If the user would like this ADSL router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices, select the radio box **Enable DHCP server on the LAN** to enter the starting IP address and end IP address and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from the remote DHCP server. The remote DHCP server will provide the IP address.

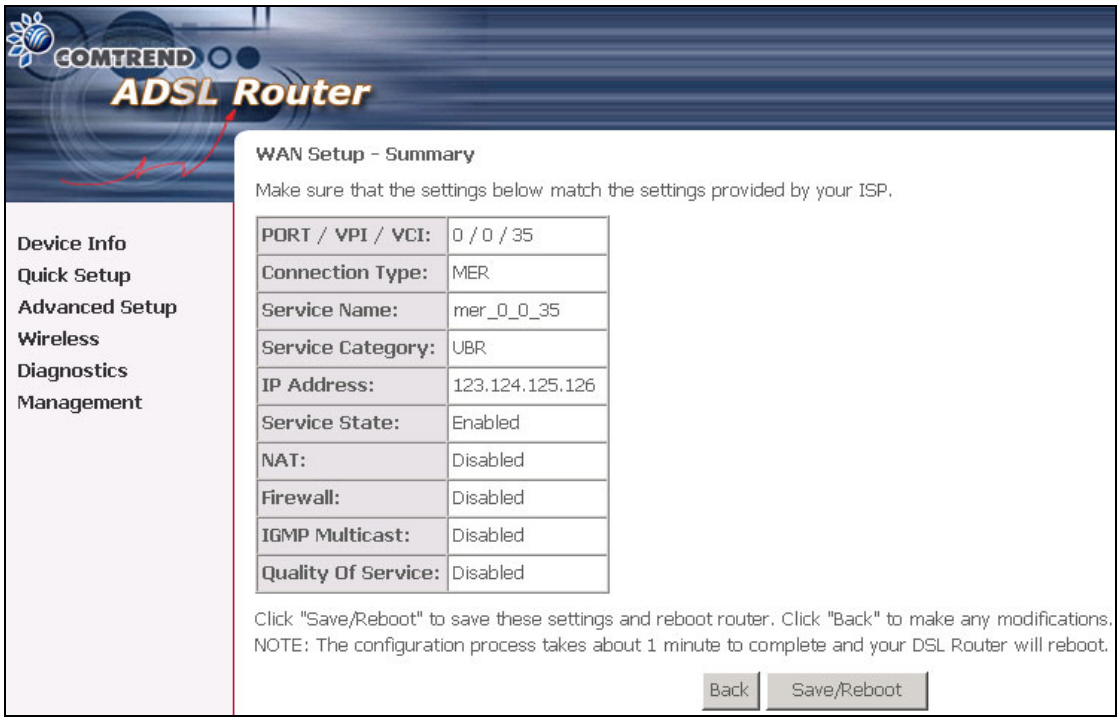
NOTE:	If NAT is enabled, **Enable DHCP Server Relay** won't display.

To configure a secondary IP address for the LAN port, click the box as shown below.



Step 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown), input a new SSID (if desired) and click **Next**.

The following screen will display.

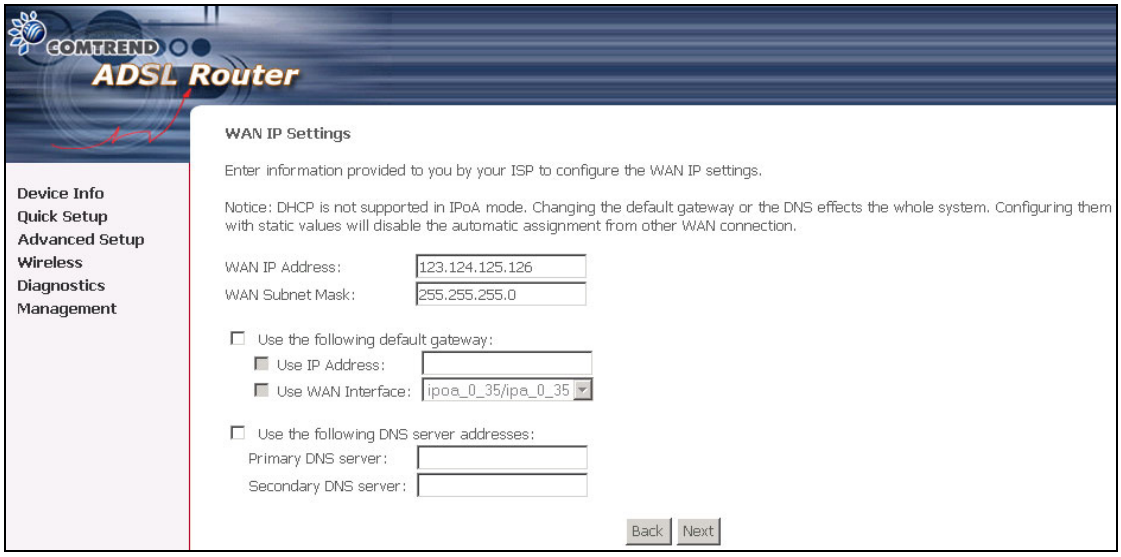


Step 8: The WAN Setup-Summary screen presents the entire configuration summary. After clicking **Save/Reboot**, the router will save the configuration to flash memory, and reboot. Click **Back** if you wish to modify the settings. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the **Device Info** screen automatically. The router is ready for operation when the LED indicators display as described in Chapter 1.3.

4.2.3 IP Over ATM

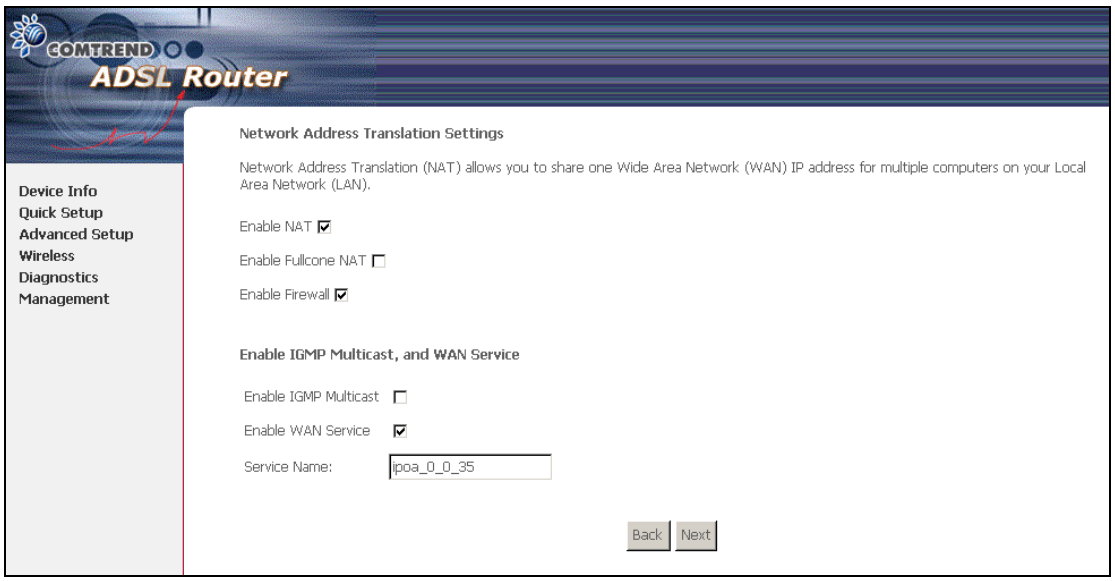
Step 4: Select the IP over ATM (IPoA) radio button and click **Next**.

The following screen appears.



NOTE:	DHCP is not supported over IPoA. The user must enter the IP address or WAN interface for the default gateway setup and the DNS server addresses provided by the ISP.

Step 5: Click **Next**. The following screen appears.



Enable NAT checkbox

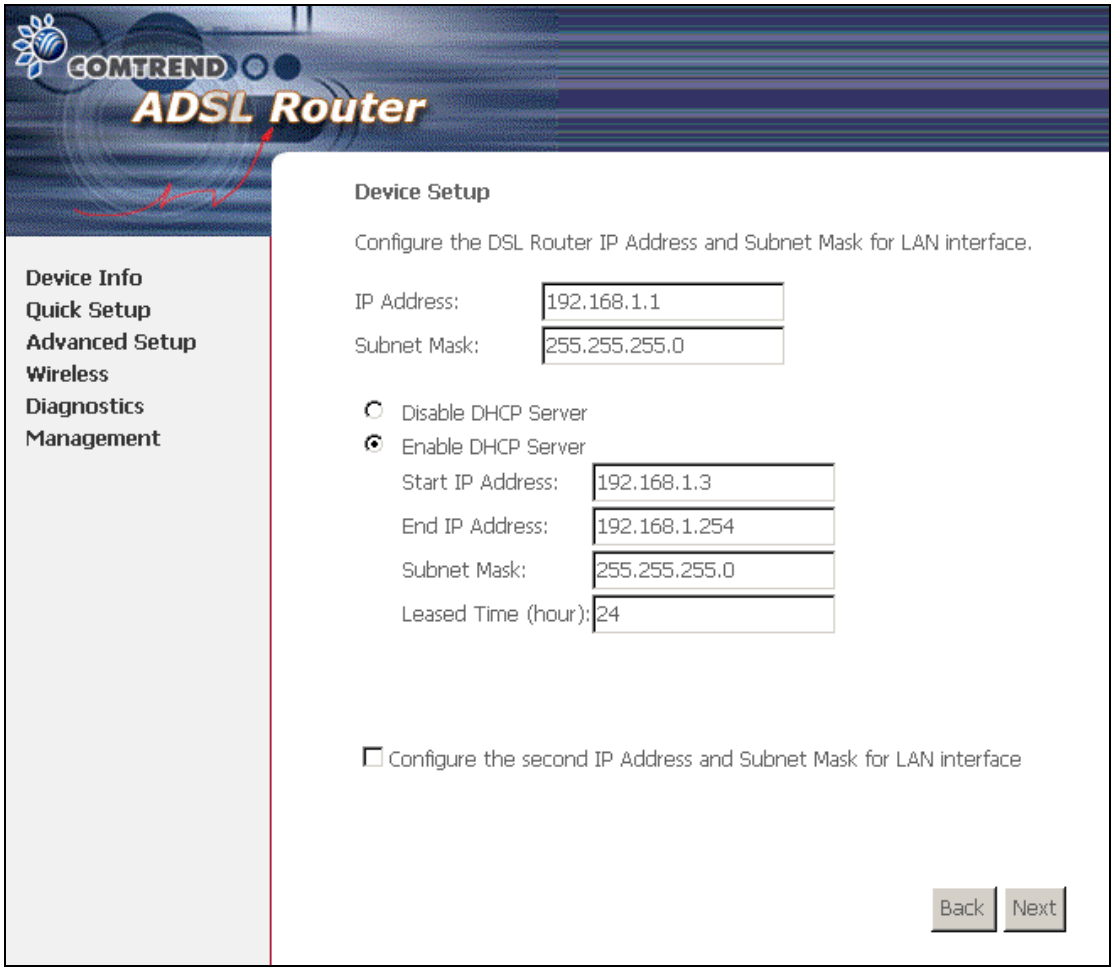
If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu on the left side main panel will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox should be de-selected. When the system comes back after reboot, the NAT submenu will not be displayed on the left main panel.

Enable Fullcone NAT: This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

Enable Firewall checkbox

If the firewall checkbox is selected, the Security submenu on the left side main panel will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Security submenu will not be displayed on the left main panel.

Step 6: Click **Next** to display the following screen.



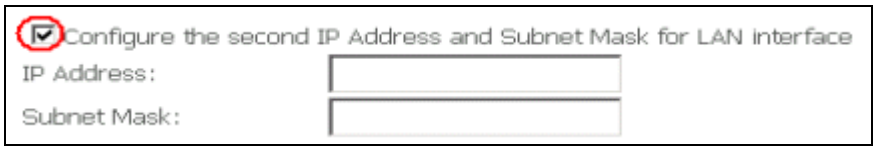
The Device Setup page allows the user to configure the LAN interface IP address and DHCP server. If the user would like this ADSL router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices. Select the button Enable DHCP server on the LAN to enter the starting IP address and end IP address and DHCP lease time.

The Device Setup page allows the user to configure the LAN interface IP address and DHCP server. If the user would like this ADSL router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices, select the radio box **Enable DHCP server on the LAN** to enter the starting IP address and end IP address and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from the remote DHCP server. The remote DHCP server will provide the IP address.

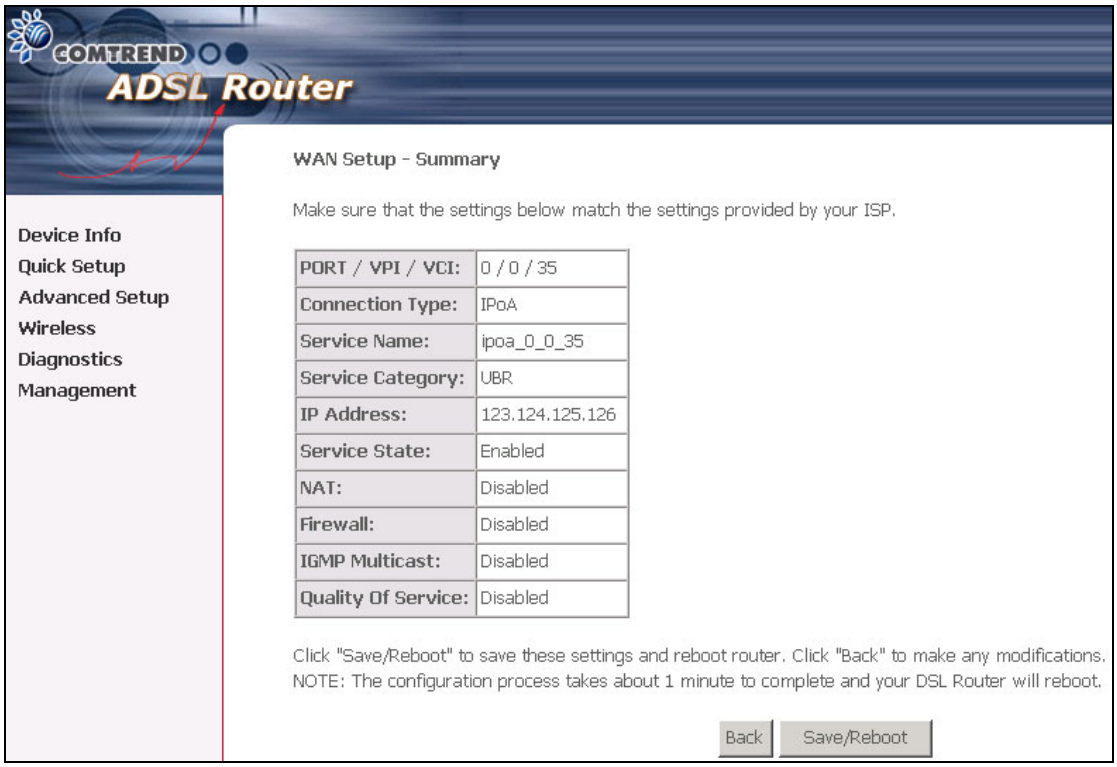
NOTE:	If NAT is enabled, **Enable DHCP Server Relay** won't display.

To configure a secondary IP address for the LAN port, click the box as shown below.



STEP 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown), input a new SSID (if desired) and click **Next**.

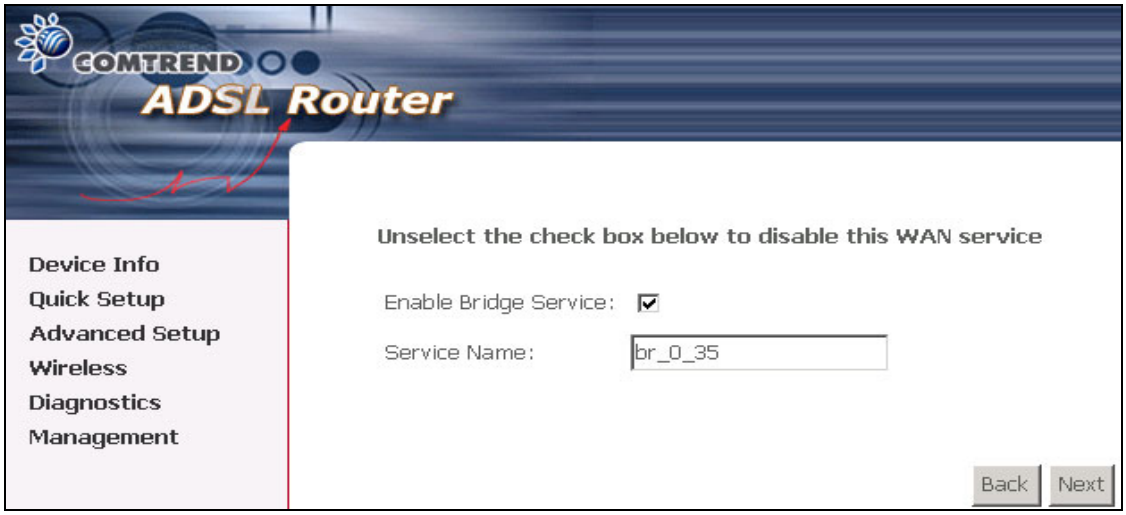
The following screen will be displayed.



Step 8: The WAN Setup-Summary screen presents the entire configuration summary. After clicking **Save/Reboot**, the router will save the configuration to the flash memory, and reboot. Click **Back** if you wish to modify the settings. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the **Device Info** page automatically. The router is ready for operation when the LED indicators display as described in Chapter 1.3.

4.2.4 Bridging

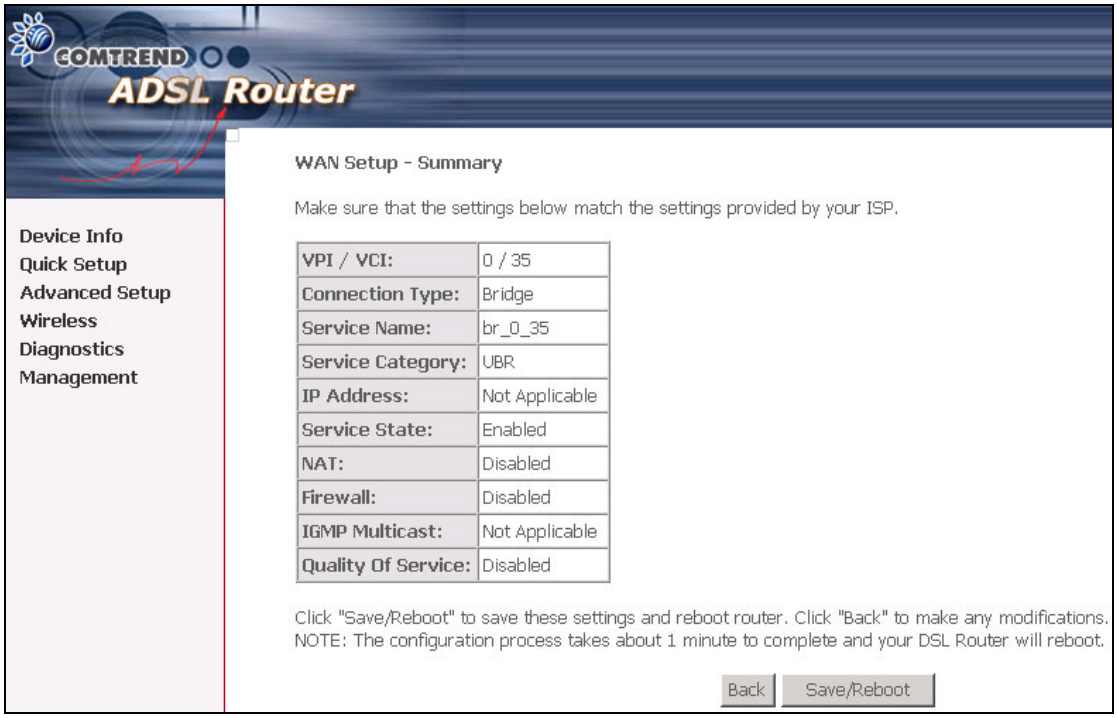
Step 4: Select the Bridging radio button and click **Next**. The following screen appears. To use the bridge service, tick the **Enable Bridge Service** checkbox and enter a service name (user defined).



Step 5: Click the **Next** button to continue. Enter the IP address for the LAN interface. The default IP address is 192.168.1.1. The LAN IP interface in bridge operating mode is needed for local users to manage the ADSL router. Notice that there is no IP address for the WAN interface in bridge mode, and the remote technical support cannot access the ADSL router.

STEP 6: Click **Next** to continue. To enable the wireless function, select the radio button (as shown), input a new SSID (if desired) and click **Next**.

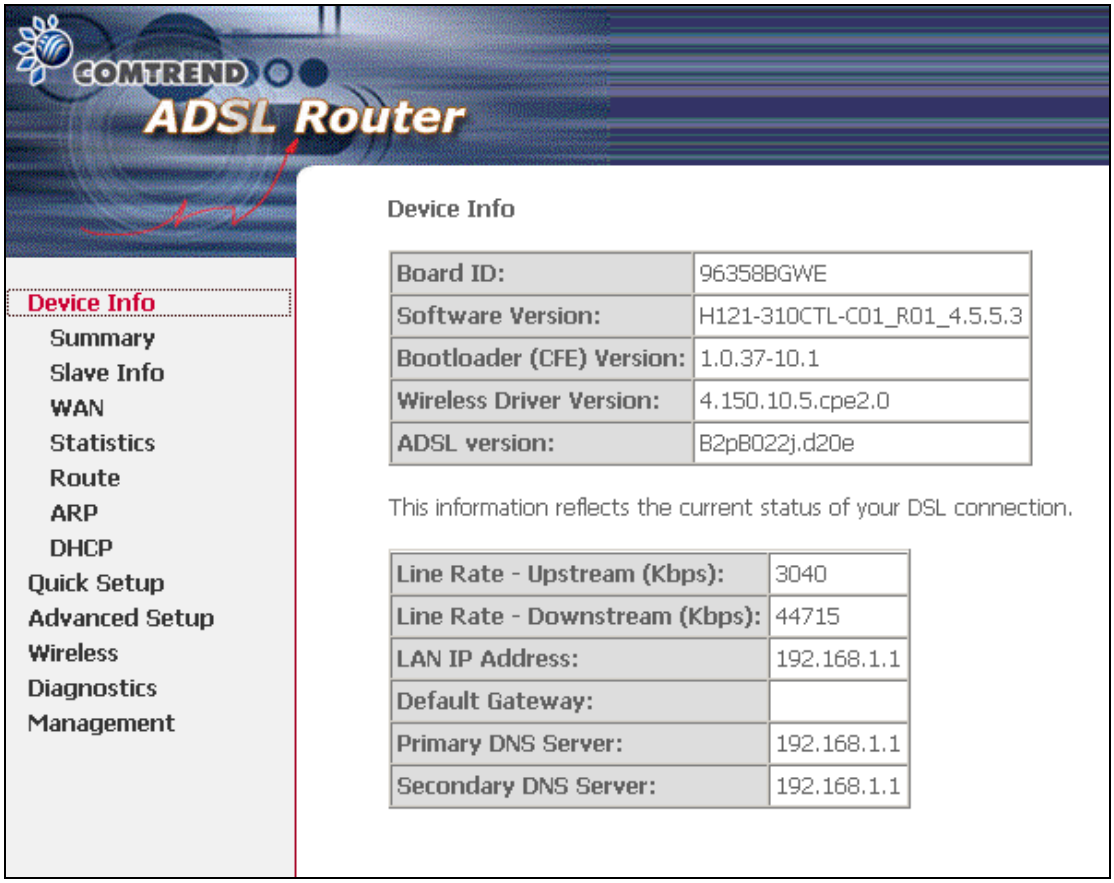
The following screen will be displayed.



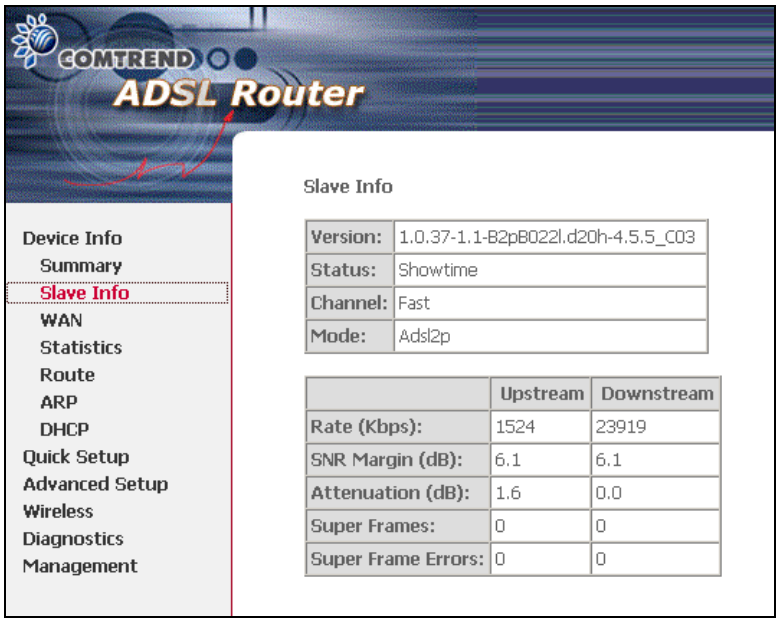
Step 7: The WAN Setup-Summary screen presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.

Chapter 5 Device Info

Select **Device Info** from the main menu to display Summary information as below.

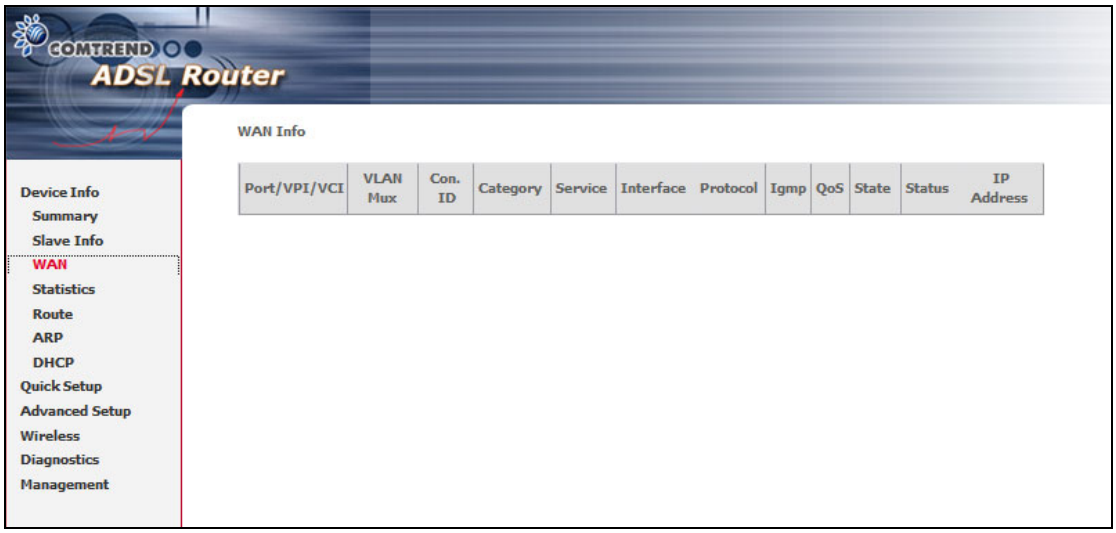


NOTE: The screen above gives a status summary for **ADSL1**. For the status of **ADSL2** consult the next selection on the menu **Slave Info**, as shown.



5.1 WAN

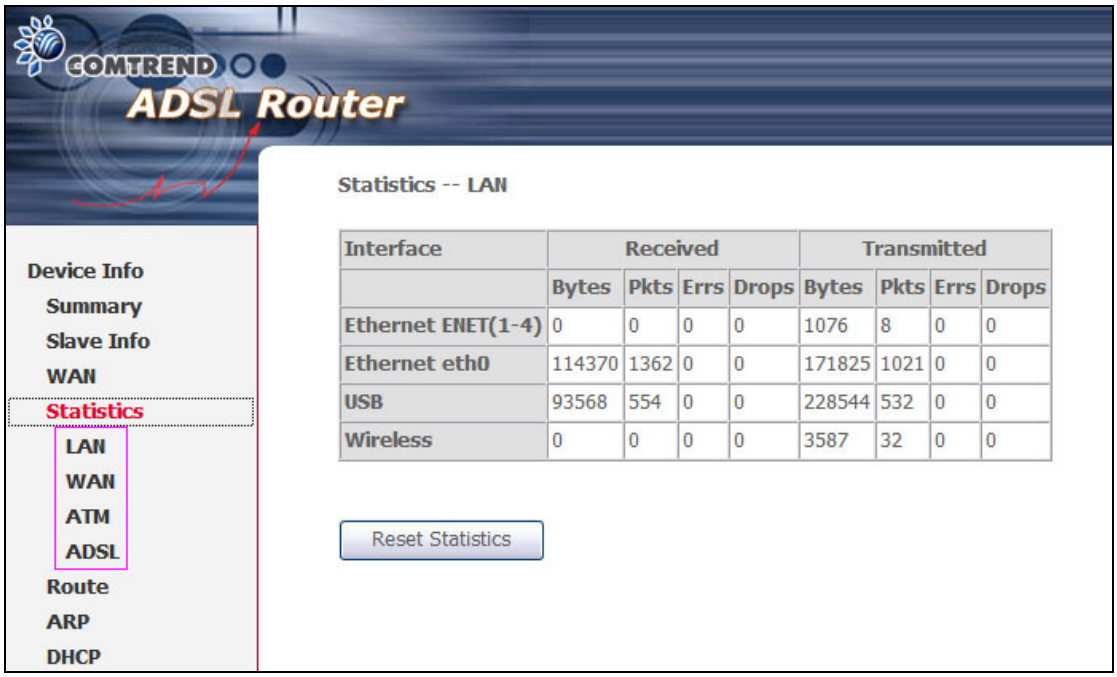
Select WAN from the Device Info menu to display the status of all configured PVC(s).



Port/VPI/VCI	Shows the values of the ATM Port/VPI/VCI
VLAN Mux	Shows 802.1Q VLAN ID
Con. ID	Shows the connection ID
Category	Shows the ATM service classes
Service	Shows the name for WAN connection
Interface	Shows connection interfaces
Protocol	Shows the connection type, such as PPPoE, PPPoA, etc.
IGMP	Shows the statue of the IGMP function
State	Shows the connection state of the WAN connection
Status	Lists the status of the ADSL link
IP Address	Shows IP address for WAN interface

5.2 Statistics

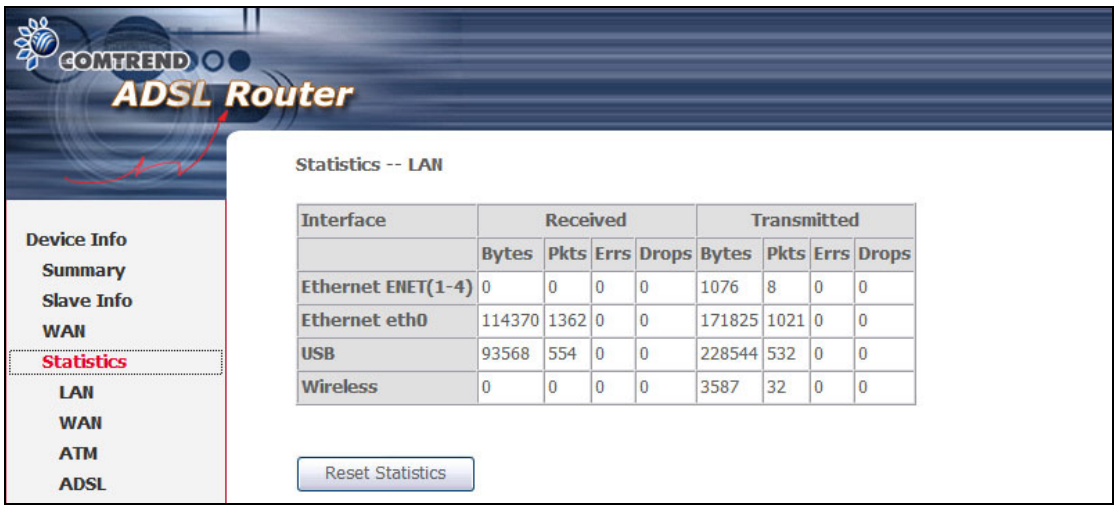
Selection of the Statistics screen provides statistics for the Network Interface of LAN, WAN, ATM and ADSL. All statistics screens are updated every 15 seconds.



eth0: Communication interface between internal CPUs.

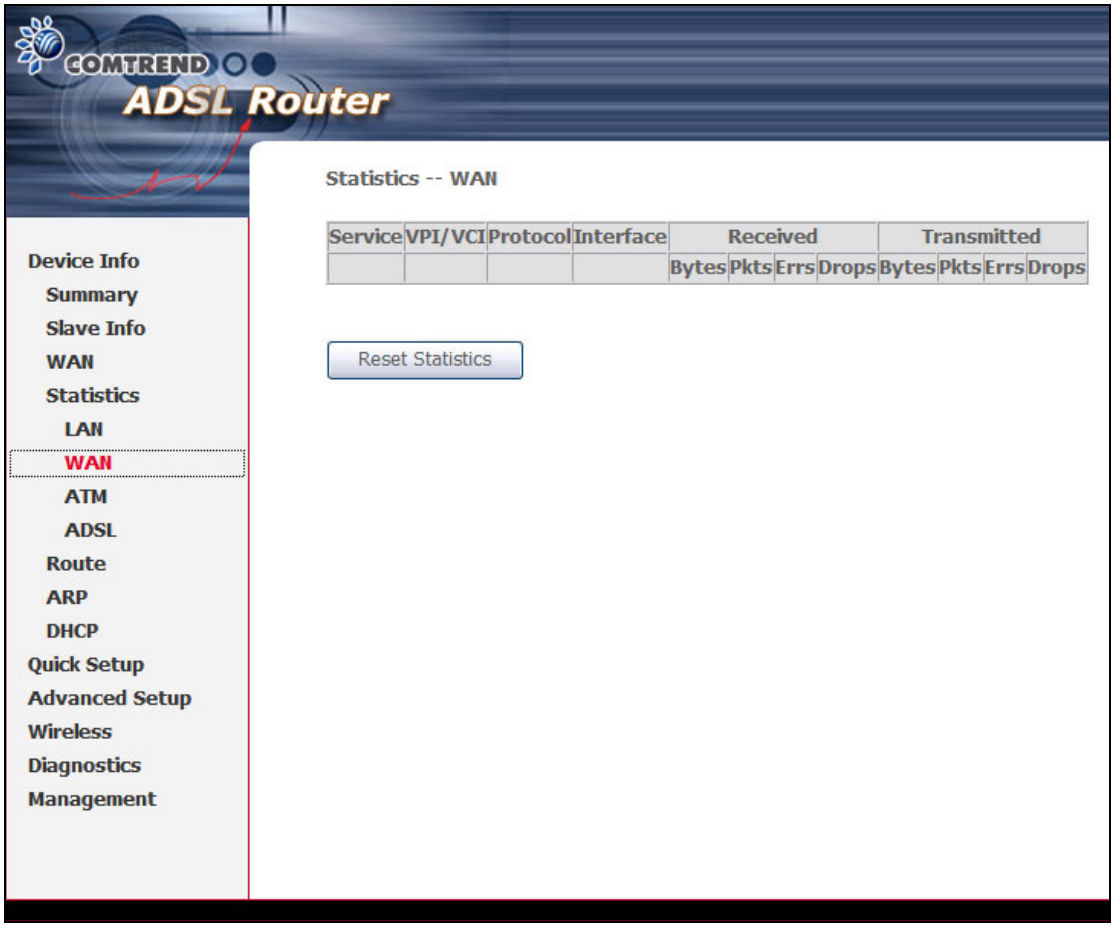
5.2.1 LAN Statistics

The Network Statistics screen shows interface statistics for Ethernet and Wireless interfaces. (The Network Statistics screen shows interface statistics for LAN of Ethernet interface. Here provides byte transfer, packet transfer, Error and Drop statistics for the LAN interface.)



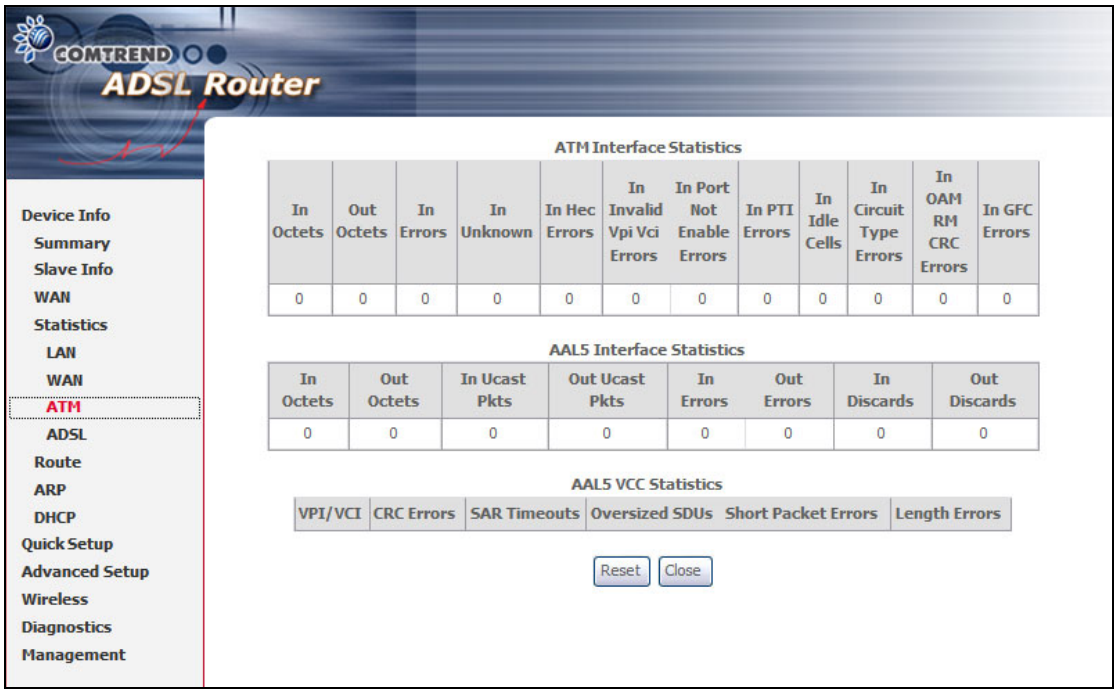
eth0: Communication interface between internal CPUs.

5.2.2 WAN Statistics



Service	Shows the service type
VPI/VCI	Shows the values of the ATM VPI/VCI
Protocol	Shows the connection type, such as PPPoE, PPPoA, etc.
Interface	Shows connection interfaces
Received/Transmitted - Bytes - Pkts - Errs - Drops	Rx/TX (receive/transmit) packet in Byte Rx/TX (receive/transmit) packets Rx/TX (receive/transmit) the packets which are errors, Rx/TX (receive/transmit) the packets which are dropped

5.2.3 ATM statistics



Field	Description
In Octets	Number of received octets over the interface
Out Octets	Number of transmitted octets over the interface
In Errors	Number of cells dropped due to uncorrectable HEC errors
In Unknown	Number of received cells discarded during cell header validation, including cells with unrecognized VPI/VCI values, and cells with invalid cell header patterns. If cells with undefined PTI values are discarded, they are also counted here.
In Hec Errors	Number of cells received with an ATM Cell Header HEX error
In Invalid Vpi Vci Errors	Number of cells received with an unregistered VCC address.
In Port Not Enabled Errors	Number of cells received on a port that has not been enabled.
In PTI Errors	Number of cells received with an ATM header Payload Type Indicator (PTI) error
In Idle Cells	Number of idle cells received
In Circuit Type Errors	Number of cells received with an illegal circuit type
In Oam RM CRC Errors	Number of OAM and RM cells received with CRC errors
In GFC Errors	Number of cells received with a non-zero GFC.

ATM AAL5 Layer Statistics over ADSL interface

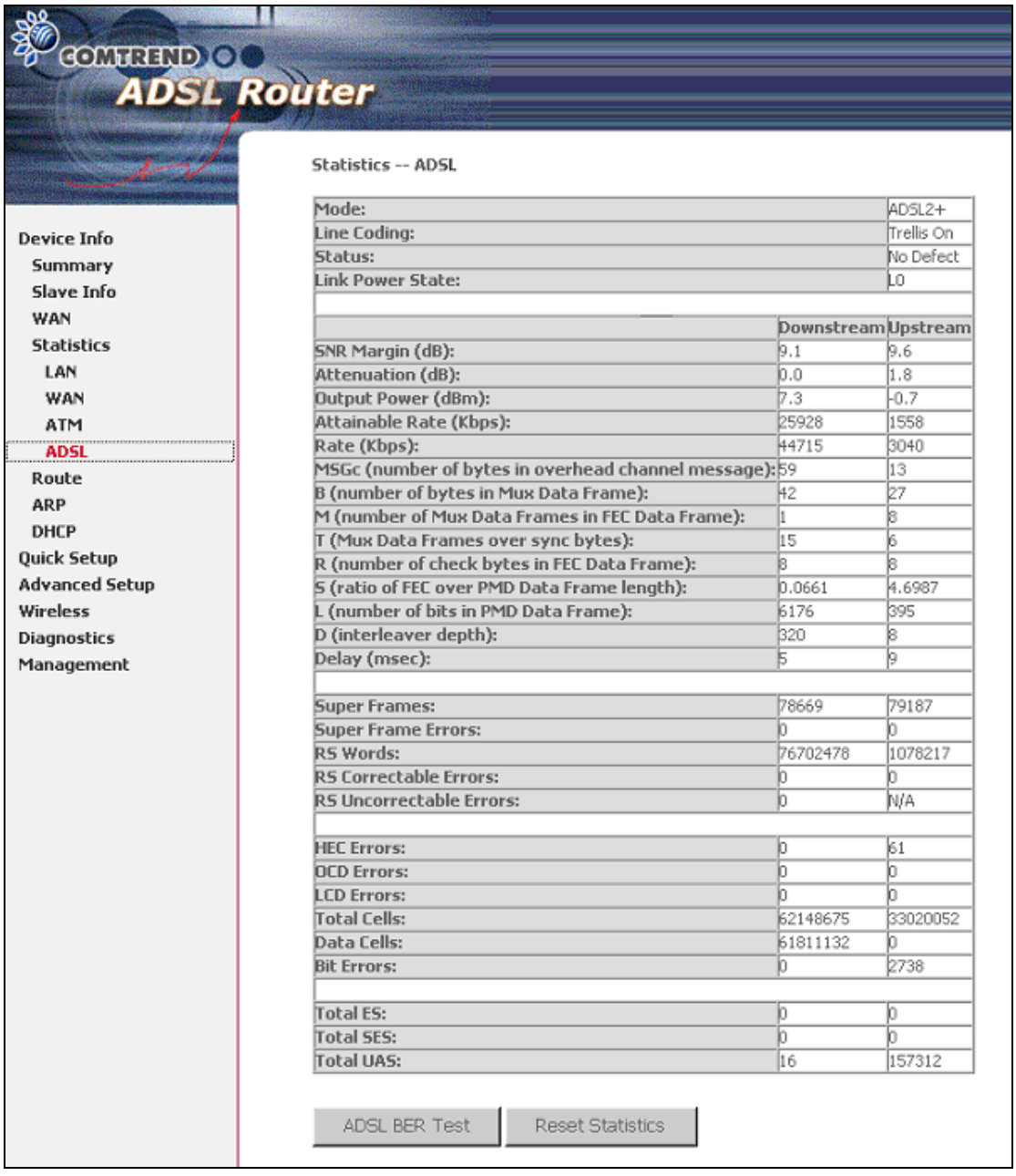
Field	Description
In Octets	Number of received AAL5/AAL0 CPCS PDU octets
Out Octets	Number of received AAL5/AAL0 CPCS PDUs octets transmitted
In Ucst Pkts	Number of received AAL5/AAL0 CPCS PDUs passed to a higher-layer for transmission
Out Ucast Pkts	Number of received AAL5/AAL0 CPCS PDUs received from a higher layer for transmissions
In Errors	Number of received AAL5/AAL0 CPCS PDUs received that contain an error. The types of errors counted include CRC-32 errors.
Out Errors	Number of received AAL5/AAL0 CPCS PDUs that could be transmitted due to errors.
In Discards	Number of received AAL5/AAL0 CPCS PDUs discarded due to an input buffer overflow condition.
Out Discards	This field is not currently used

ATM AAL5 Layer Statistics for each VCC over ADSL interface

Field	**Description**
CRC Errors	Number of PDUs received with CRC-32 errors
SAR TimeOuts	Number of partially re-assembled PDUs which were discarded because they were not fully re-assembled within the required period of time. If the re-assembly time is not supported then, this object contains a zero value.
Over Sized SDUs	Number of PDUs discarded because the corresponding SDU was too large
Short Packets Errors	Number of PDUs discarded because the PDU length was less than the size of the AAL5 trailer
Length Errors	Number of PDUs discarded because the PDU length did not match the length in the AAL5 trailer

5.2.4 ADSL Statistics

The following graphic shows the ADSL Network Statistics screen. Within the ADSL Statistics window, a bit Error Rate Test can be started using the ADSL BER Test button. The Reset button resets the statistics.



Mode:		ADSL2+
Line Coding:		Trellis On
Status:		No Defect
Link Power State:		L0
	Downstream	Upstream
SNR Margin (dB):	9.1	9.6
Attenuation (dB):	0.0	1.8
Output Power (dBm):	7.3	-0.7
Attainable Rate (Kbps):	25928	1558
Rate (Kbps):	44715	3040
MSGc (number of bytes in overhead channel message):	59	13
B (number of bytes in Mux Data Frame):	42	27
M (number of Mux Data Frames in FEC Data Frame):	1	8
T (Mux Data Frames over sync bytes):	15	6
R (number of check bytes in FEC Data Frame):	8	8
S (ratio of FEC over PMD Data Frame length):	0.0661	4.6987
L (number of bits in PMD Data Frame):	6176	395
D (interleaver depth):	320	8
Delay (msec):	5	9
Super Frames:	78669	79187
Super Frame Errors:	0	0
RS Words:	76702478	1078217
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	N/A
HEC Errors:	0	61
OCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	62148675	33020052
Data Cells:	61811132	0
Bit Errors:	0	2738
Total ES:	0	0
Total SES:	0	0
Total UAS:	16	157312

NOTE: This display is for **ADSL1**; please refer to Appendix A for **ADSL2**.

Consult the table that follows for descriptions of each field.

Field	Description
Mode	Line Coding format, that can be selected G.dmt, G.lite, T1.413, ADSL2
Type	Channel type Interleave or Fast
Line Coding	Trellis On/Off
Status	Lists the status of the ADSL link
Link Power State	Link output power state.
SNR Margin (dB)	Signal to Noise Ratio (SNR) margin
Attenuation (dB)	Estimate of average loop attenuation in the downstream direction.
Output Power (dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rate.

In ADSL2+ mode the following fields are inserted here.

MSGc	Number of bytes in overhead channel message
B	Number of bytes in Mux Data Frame
M	Number of Mux Data Frames in FEC Data Frame
T	Max Data Frames over sync bytes
R	Number of check bytes in FEC Data Frame
S	Ratio of FEC over PMD Data Frame length
L	Number of bits in PMD Data Frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)

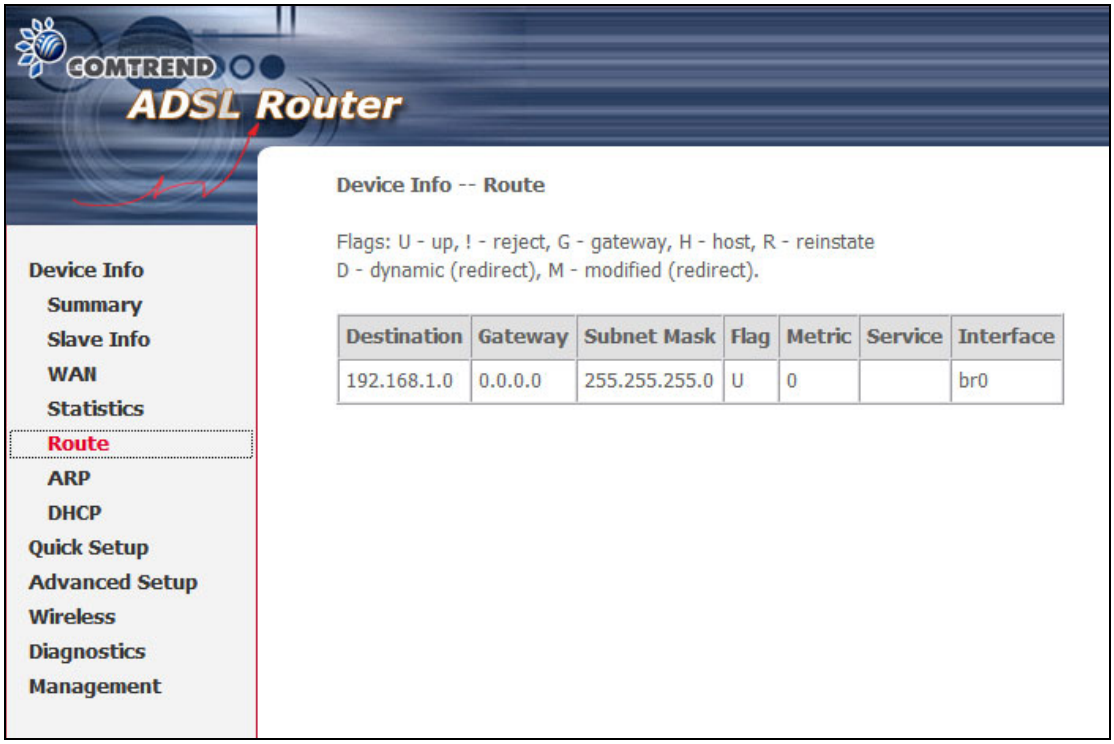
In G.DMT mode the following fields are inserted here.

K	Number of bytes in DMT frame
R	Number of check bytes in RS code word
S	RS code word size in DMT frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)

Super Frames	Total number of super frames
Super Frame Errors	Number of super frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

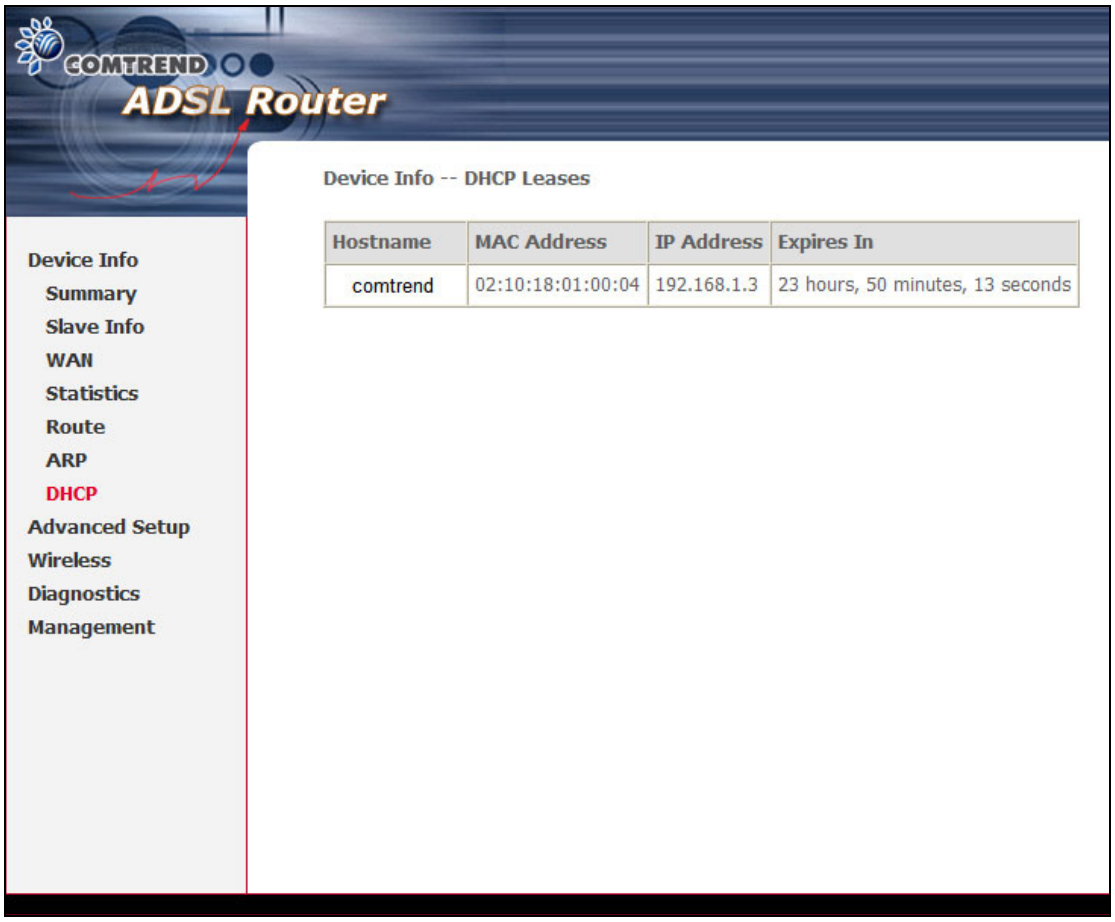
HEC Errors	Total Number of Header Error Checksum errors
OCD Errors	Total Number of out-of-cell Delineation errors
LCD Errors	Total number of Loss of Cell Delineation
Total ES:	Total Number of Errored Seconds
Total SES:	Total Number of Severely Errored Seconds
Total UAS:	Total Number of Unavailable Seconds

5.3 Route



5.4 ARP

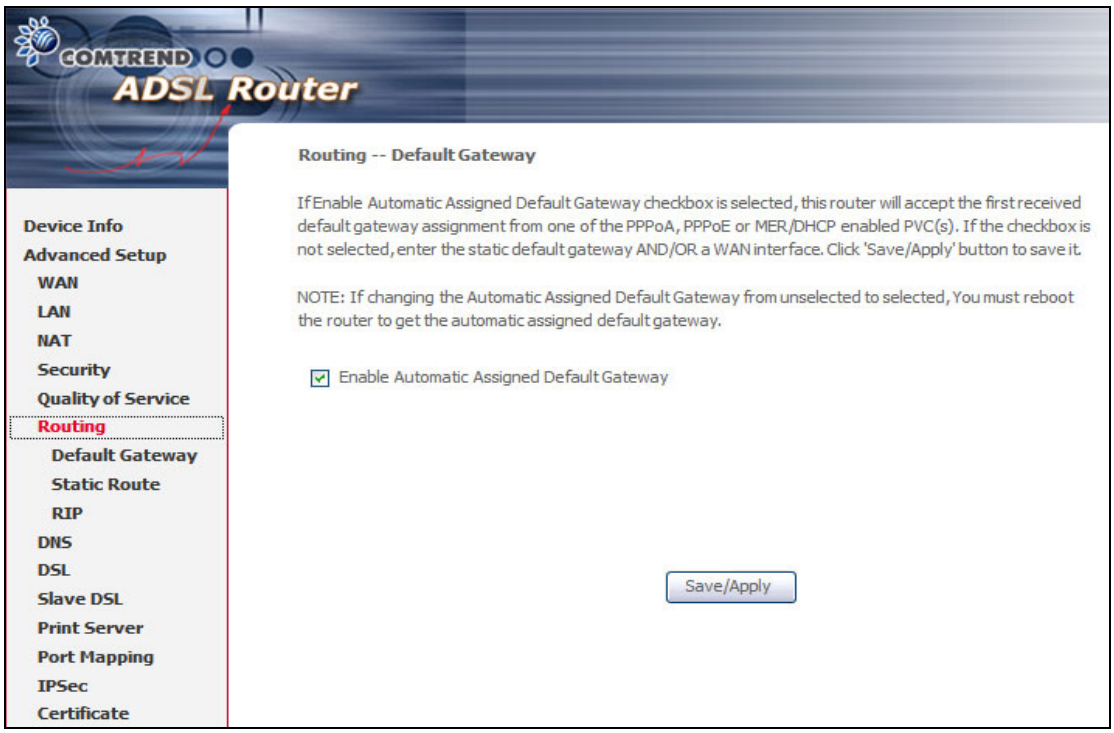
5.5 DHCP


COMTREND
ADSL Router
Device Info
Summary
Slave Info
WAN
Statistics
Route
ARP
DHCP
Advanced Setup
Wireless
Diagnostics
Management
Device Info -- DHCP Leases
Hostname
MAC Address
IP Address
Expires In
comtrend
02:10:18:01:00:04
192.168.1.3
23 hours, 50 minutes, 13 seconds

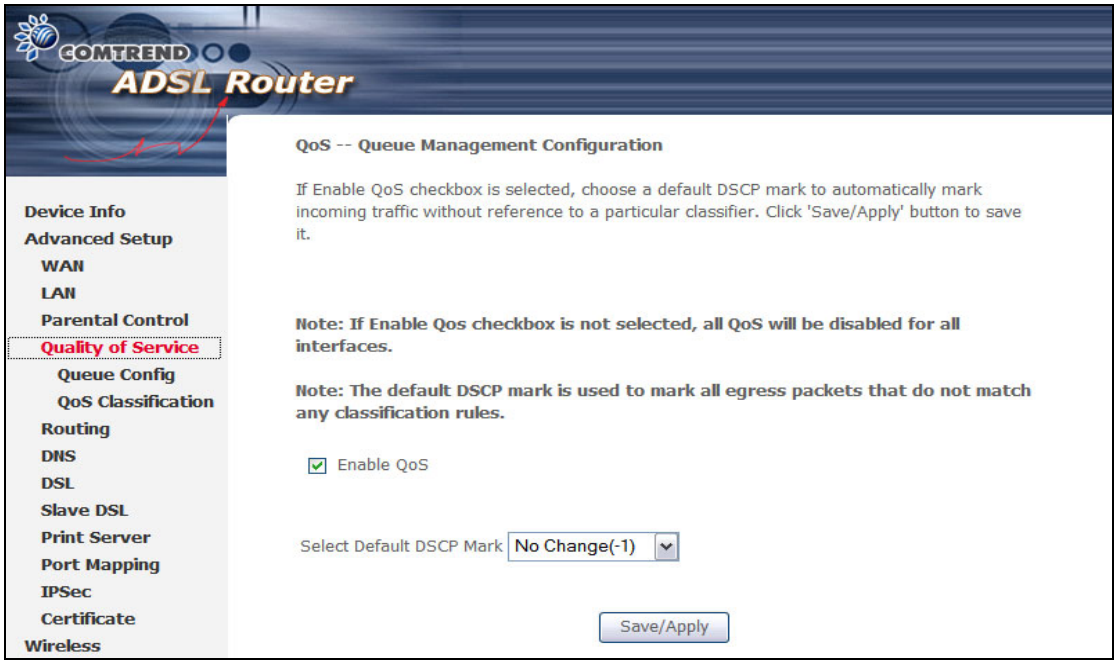
Chapter 6 Advanced Setup

This chapter explains: WAN, LAN, NAT, Security, QoS, Routing, DNS, DSL ……

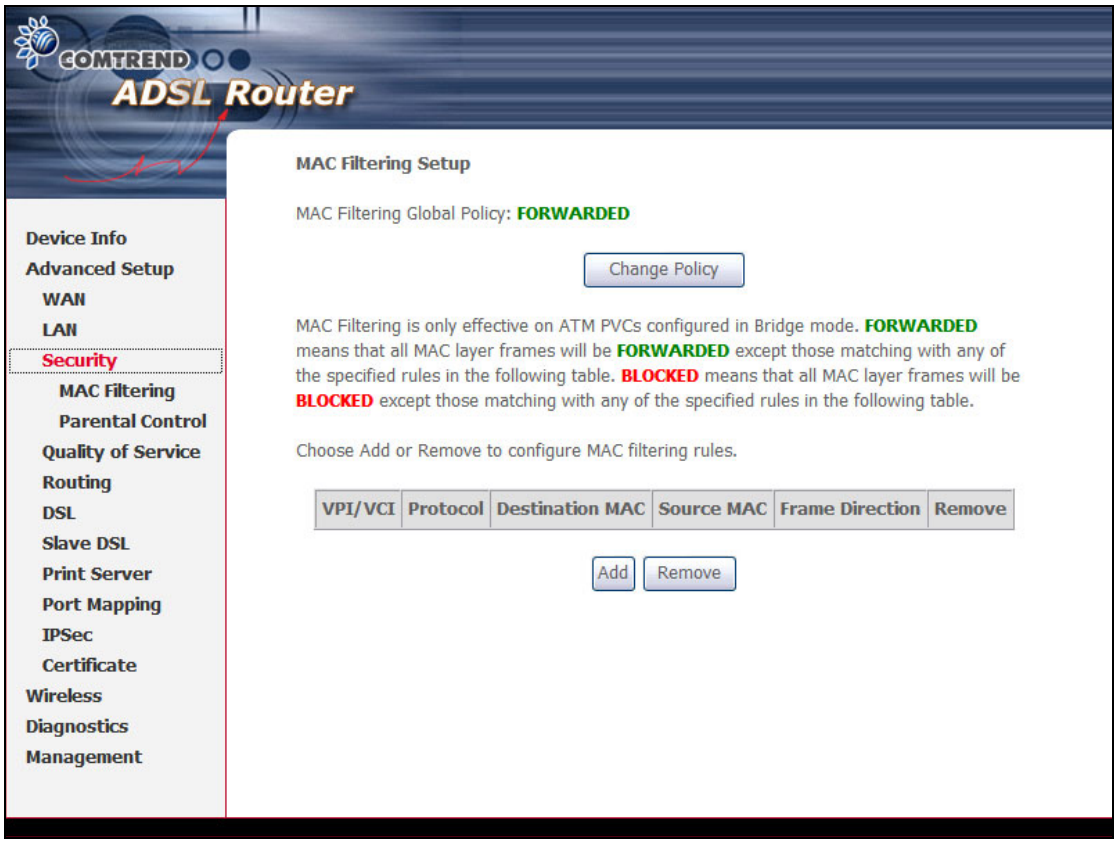
NOTE: Shown below are the menu options for each connection type.



This screenshot is for PPPoE and PPPoA encapsulations.



This screenshot is for MER and IPoA encapsulations.

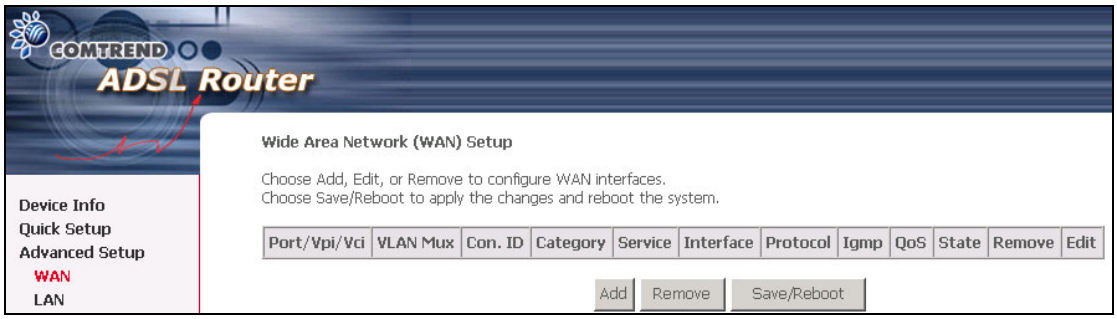


This screenshot shows MAC Filtering which is available only with Bridge connections.

6.1 WAN

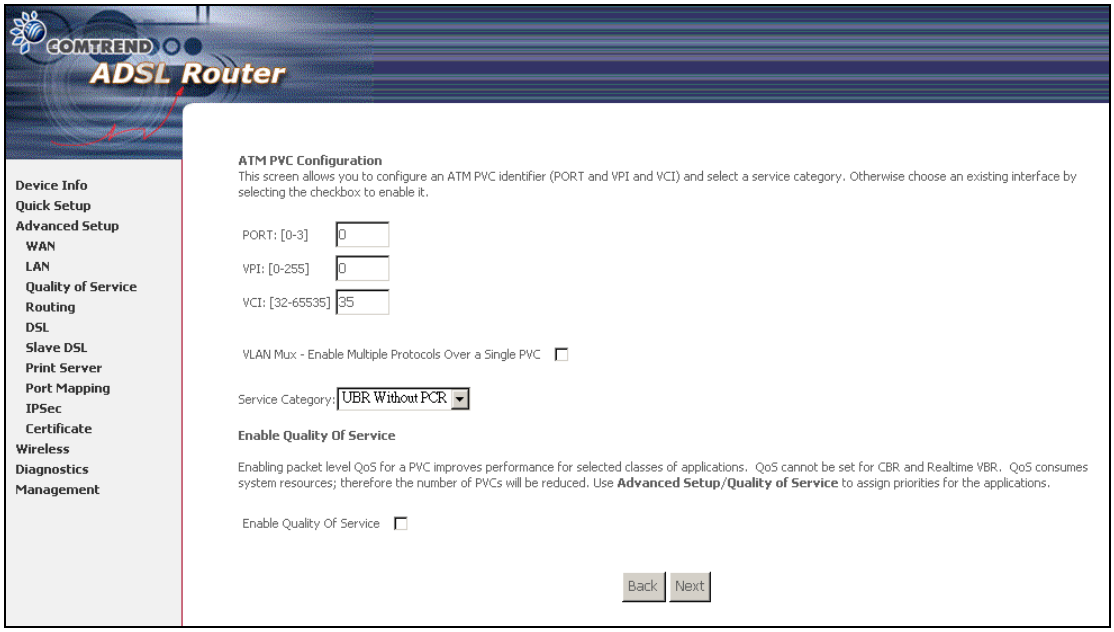
This screen allows for the advanced configuration of WAN interfaces.

STEP 1: To **Add** a new WAN connection, click the **Add** button. To edit an existing connection, click the **Edit** button next to the connection. To remove a connection select its radio button under the **Remove** column of the table and click the **Remove** button under the table.



Port/VPI/VCI	ATM Port (0-3) / VPI (0-255) / VCI (32-65535)
VLAN Mux	Shows 802.1Q VLAN ID
Con. ID	ID for WAN connection
Category	ATM service category, e.g. UBR, CBR…
Service	Name of the WAN connection
Interface	Name of the interface for WAN
Protocol	Shows bridge or router mode
IGMP	Shows enable or disable IGMP proxy
QoS	Shows enable or disable QoS
State	Shows enable or disable WAN connection

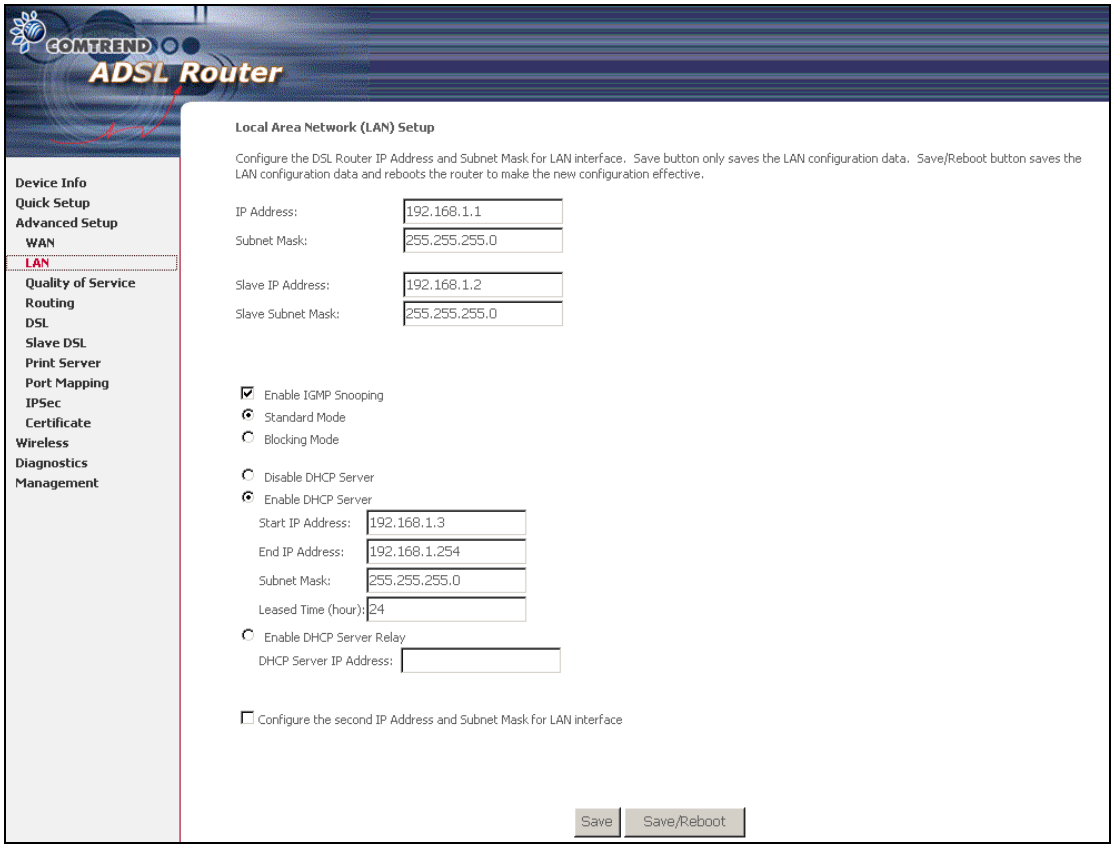
When editing or adding a connection, the screen will display as below.



To complete the **Add** or **Edit** go to STEP 2 in section 4.2 Manual Quick Setup.

6.2 LAN

Configure the ADSL Router IP Address and Subnet Mask for LAN interface. **Save** button only saves the LAN configuration data. **Save/Reboot** button saves the LAN configuration data and reboots the device to make the new configuration effective.



(Slave) IP Address: Enter the IP address for the LAN interface.

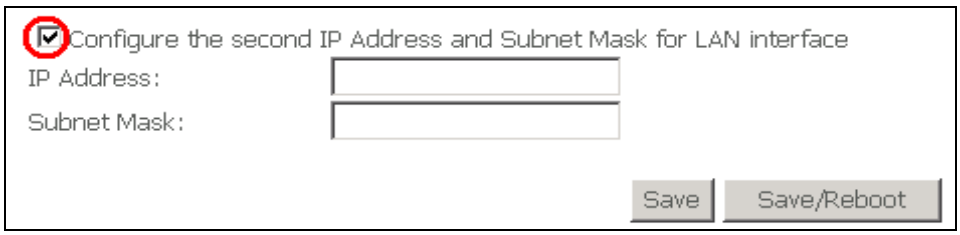
(Slave) Subnet Mask: Enter the subnet mask for the LAN interface.

Enable IGMP Snooping: Enable /Disable the function that is IGMP Snooping.

Standard Mode: In standard mode, as in all prior releases, multicast traffic will flood to all bridge ports when there is no client subscribes to any multicast group – even when IGMP snooping is enabled.

Blocking Mode: In blocking mode, the multicast data traffic will be blocked and not flood to all bridge ports when there is no client subscription to any multicast group.

To configure a secondary IP address for the LAN port, click the box as shown below.



6.3 NAT

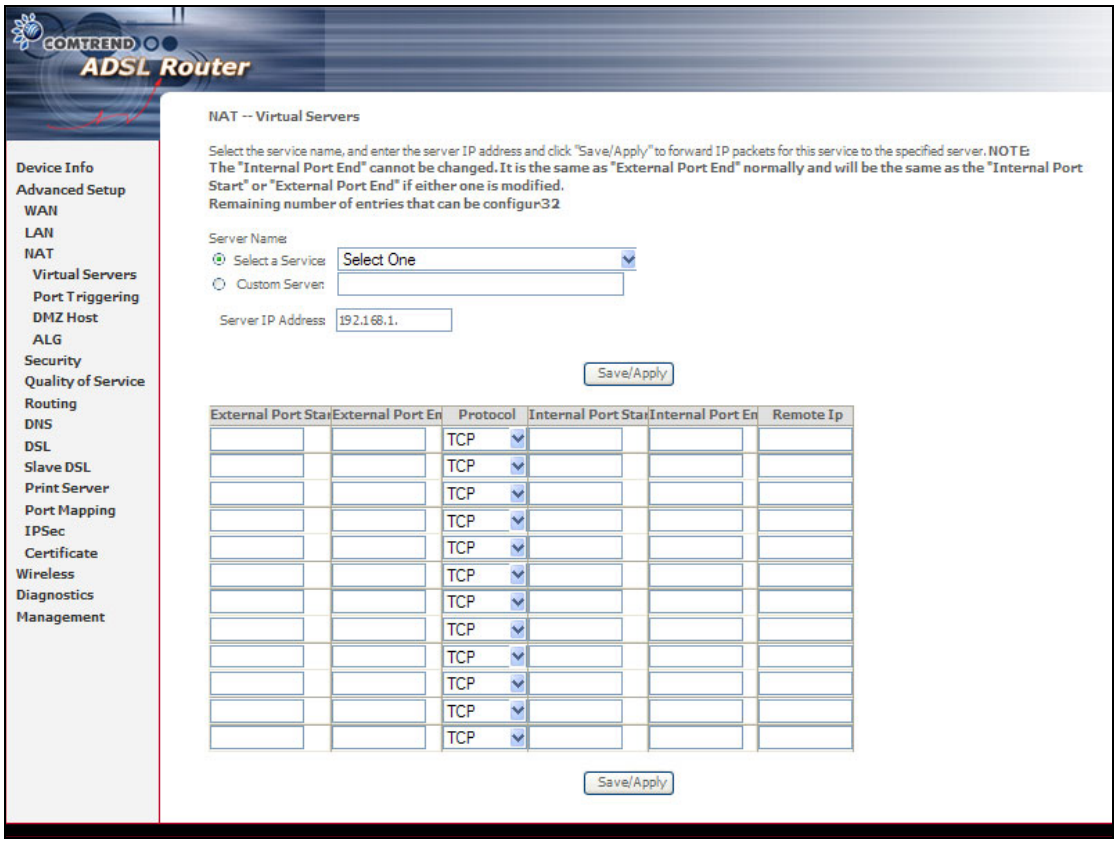
To display the NAT function, the NAT option must be enabled in WAN Setup.

6.3.1 Virtual Servers

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

To add a Virtual Server, simply click the **Add** button.

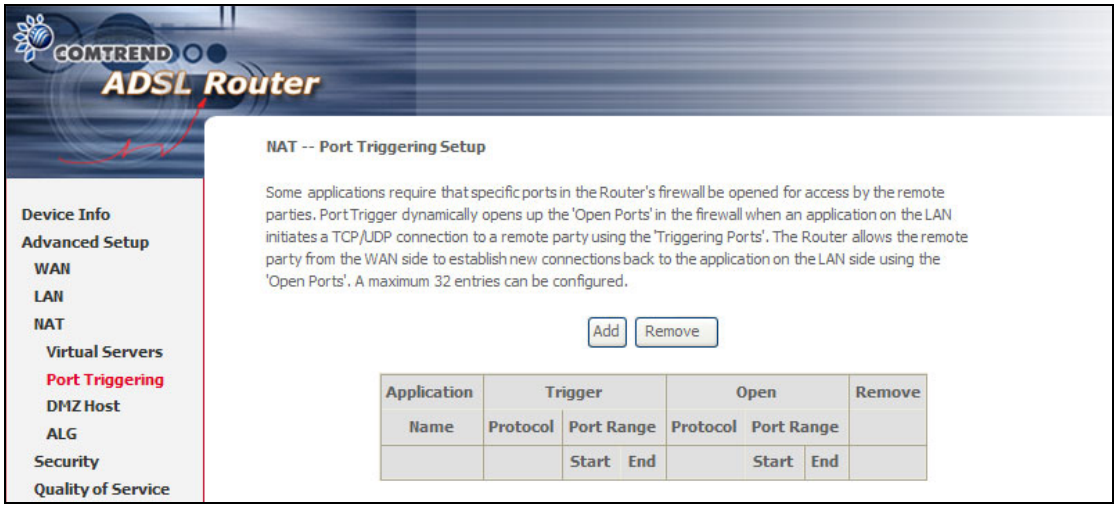
The following screen will be displayed.



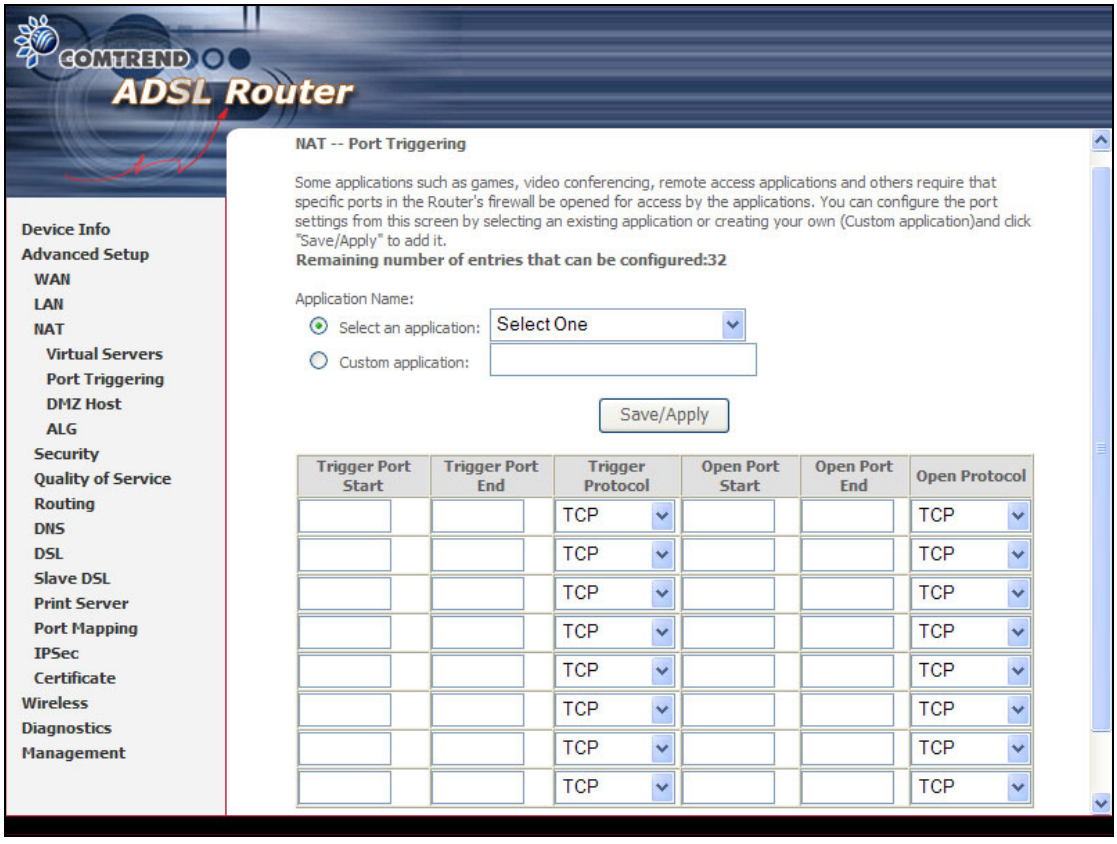
Select a Service **or** Custom Server	User should select the service from the list. **or** User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
Protocol	User can select from: TCP, TCP/UDP or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected the port ranges are automatically configured.

6.3.2 Port Triggering

Some applications require that specific ports in the router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.



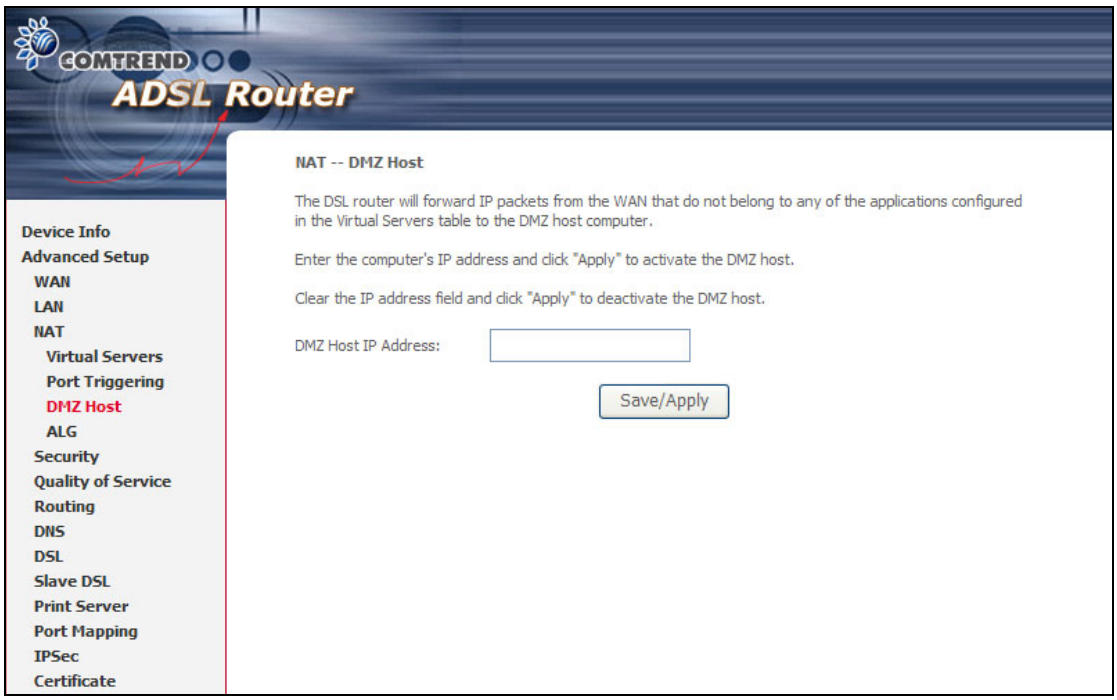
To add a Trigger Port, simply click the **Add** button. The following will be displayed.



Select an Application **Or** Custom Application	User should select the application from the list. **Or** User can enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Trigger Protocol	User can select from: TCP, TCP/UDP or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Open Protocol	User can select from: TCP, TCP/UDP or UDP.

6.3.3 DMZ Host

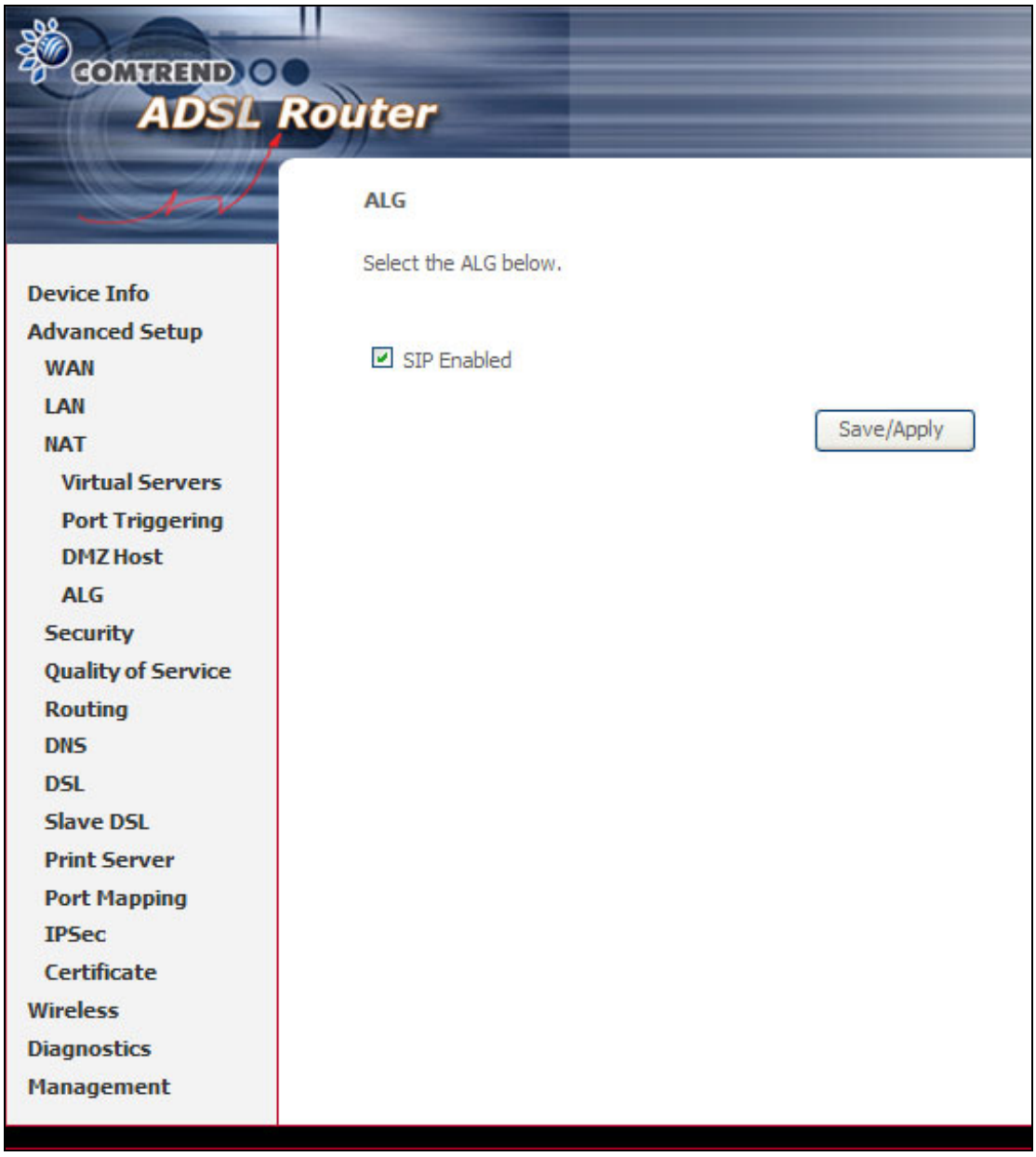
The ADSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.



Enter the computer's IP address and click "Apply" to activate the DMZ host.
Clear the IP address field and click "Apply" to deactivate the DMZ host.

6.3.4 ALG

SIP ALG is Application layer gateway. If the user has an IP phone (SIP) or VoIP gateway (SIP) behind the ADSL router, the SIP ALG can help VoIP packet passthrough the router (NAT enabled).



NOTE: SIP (Session Initiation Protocol, RFC3261) is the protocol of choice for most VoIP (Voice over IP) phones to initiate communication. This ALG is only valid for SIP protocol running UDP port 5060.

6.4 Security

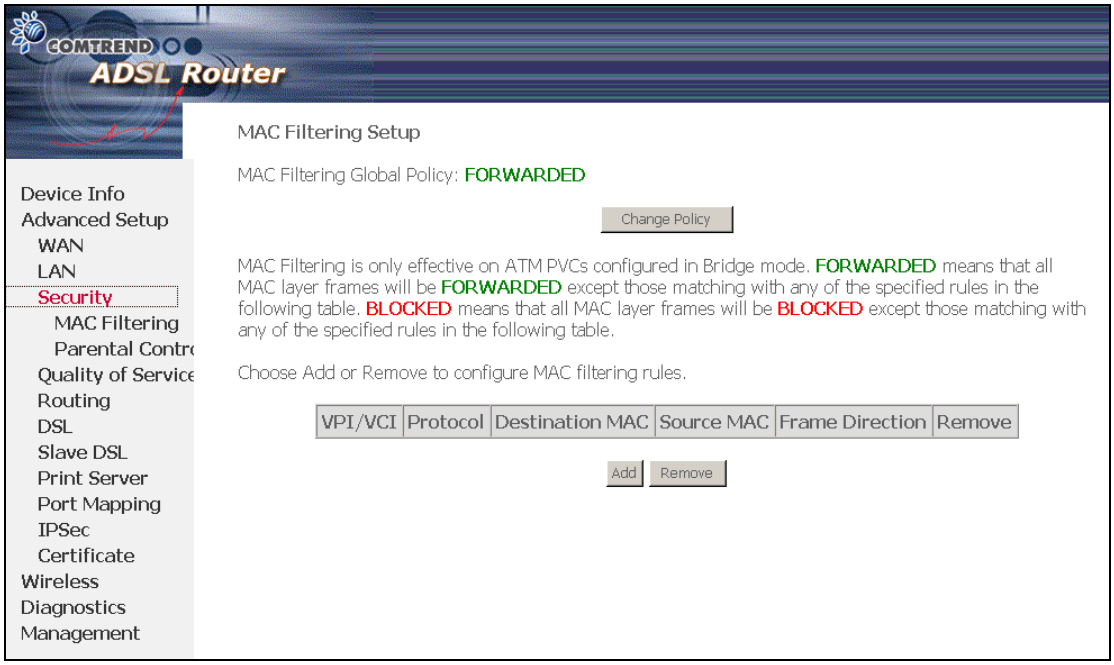
To display the Security function, the firewall option must be enabled in WAN Setup.

6.4.1 MAC Filtering

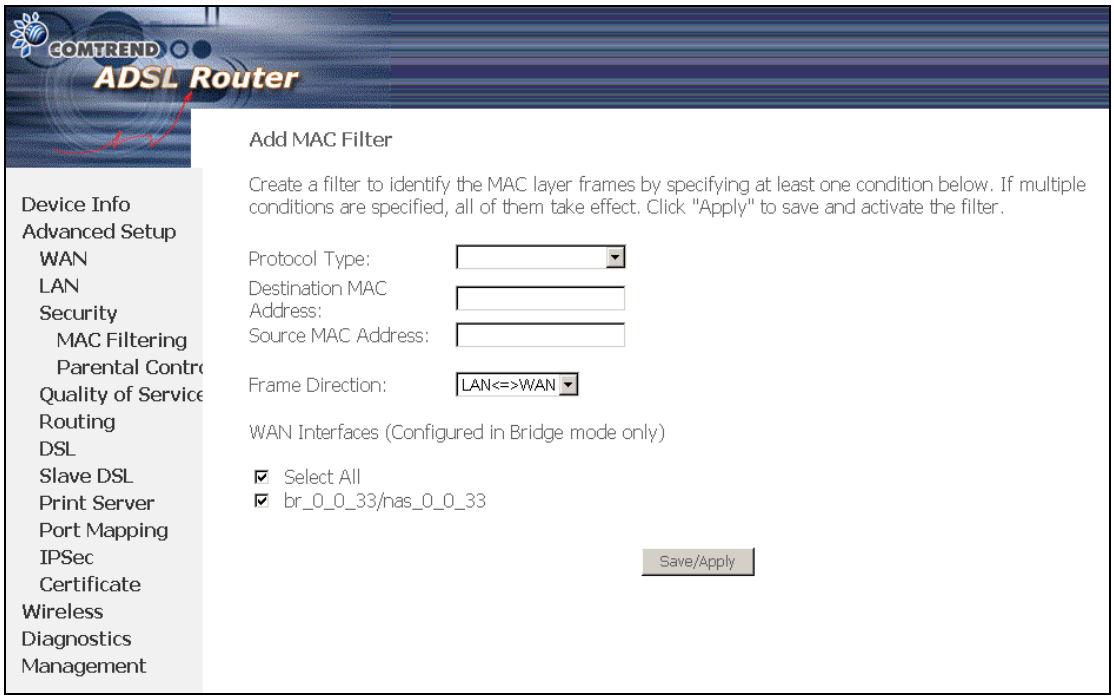
Each network device has a unique MAC address. You can block or forward the packets based on the MAC addresses. The MAC Filtering Setup screen allows for the setup of the MAC filtering policy and rules.

NOTE:	This function is only available when in bridge mode. Instead of MAC filtering, the other connection types use IP Filtering (pg. 65).

The policy **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table. The default is **FORWARDED**; this is changed by clicking the **Change Policy** button.



Choose **Add** or **Remove** to configure MAC filtering rules. The following screen pops up when you click **Add**. Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click **Save/Apply** to save and activate the filter.



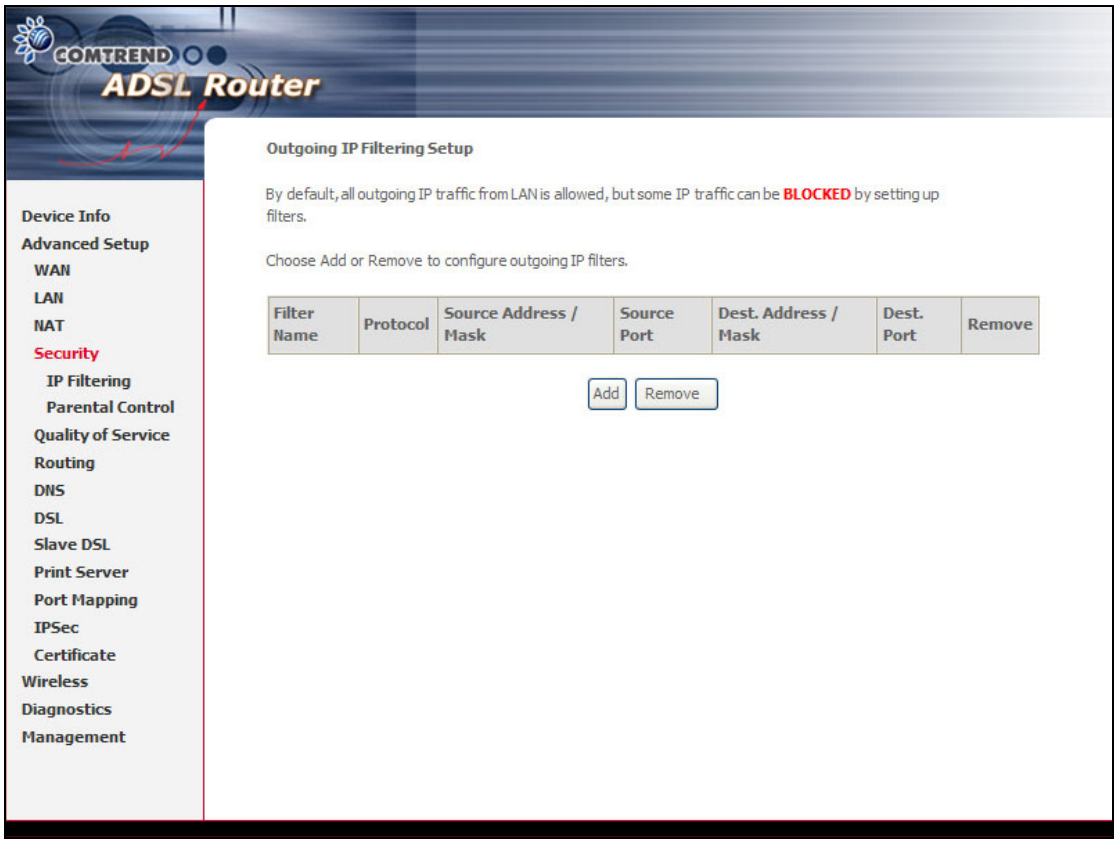
Field	Description
Protocol type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface

6.4.2 IP Filtering

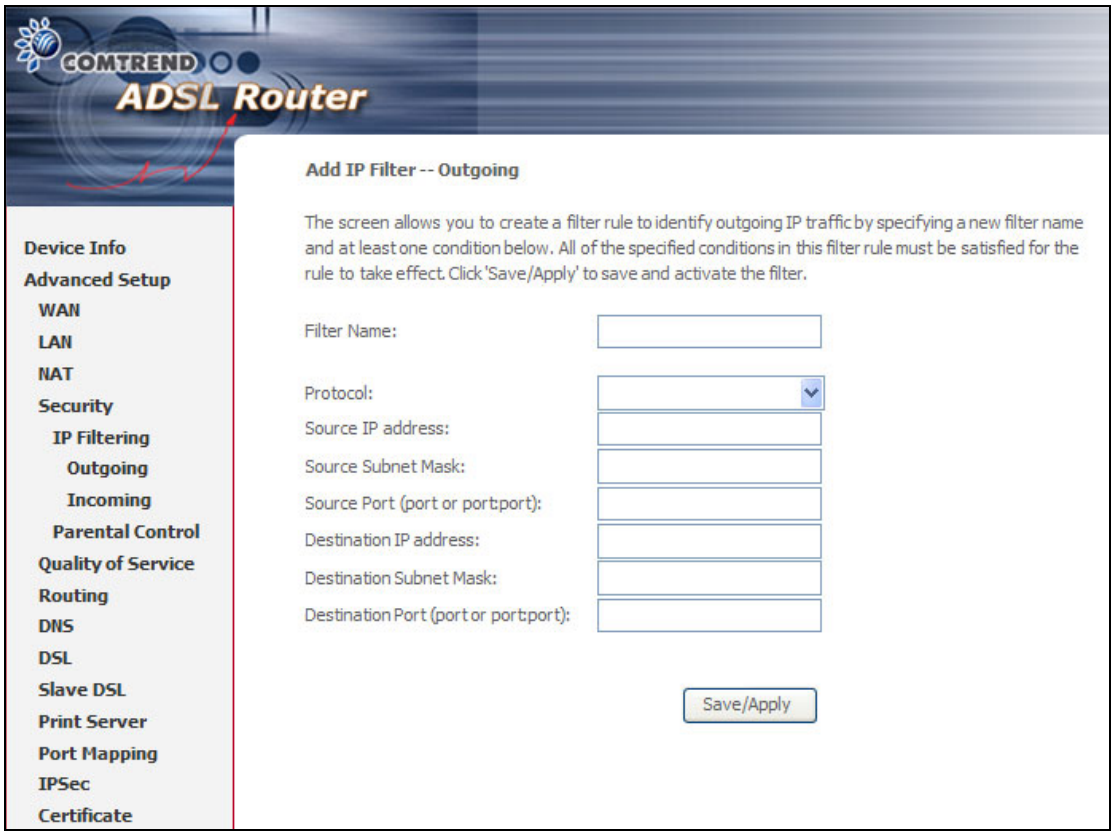
IP filtering allows you to create a filter rule to identify outgoing/incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click **Save/Apply** to save and activate the filter.

Outgoing

The default setting for all Outgoing traffic is **ACCEPTED**.



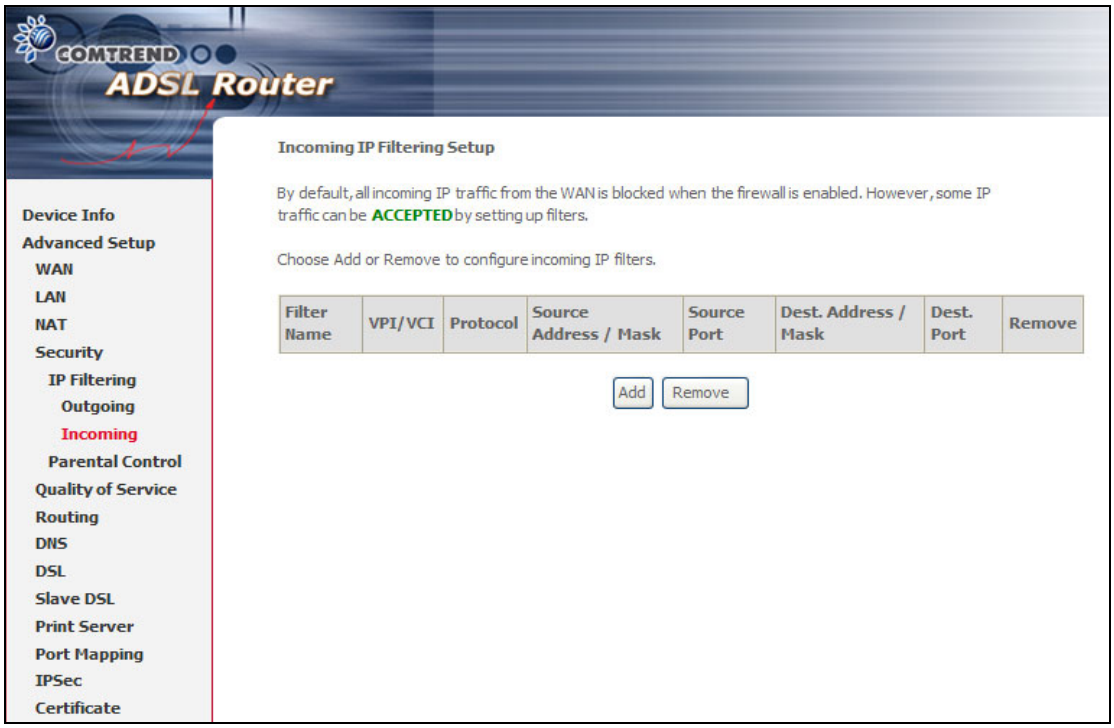
To add a filtering rule, click the **Add** button. The following screen will be displayed.



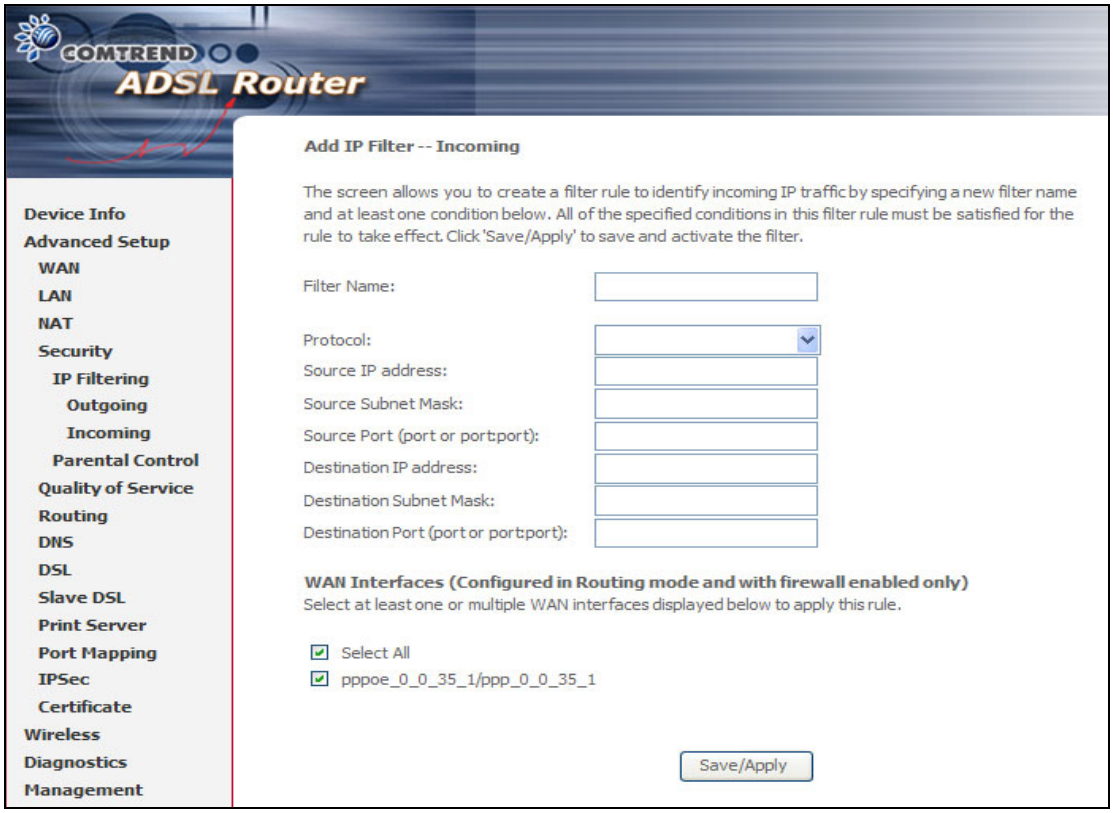
Filter Name	Type a name for the filter rule.
Protocol	User can select: TCP, TCP/UDP, UDP or ICMP.
Source IP address	Enter source IP address.
Source Subnet Mask	Enter source subnet mask.
Source Port (port or port:port)	Enter source port number.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number.

Incoming

The default setting for all Incoming traffic is Blocked.



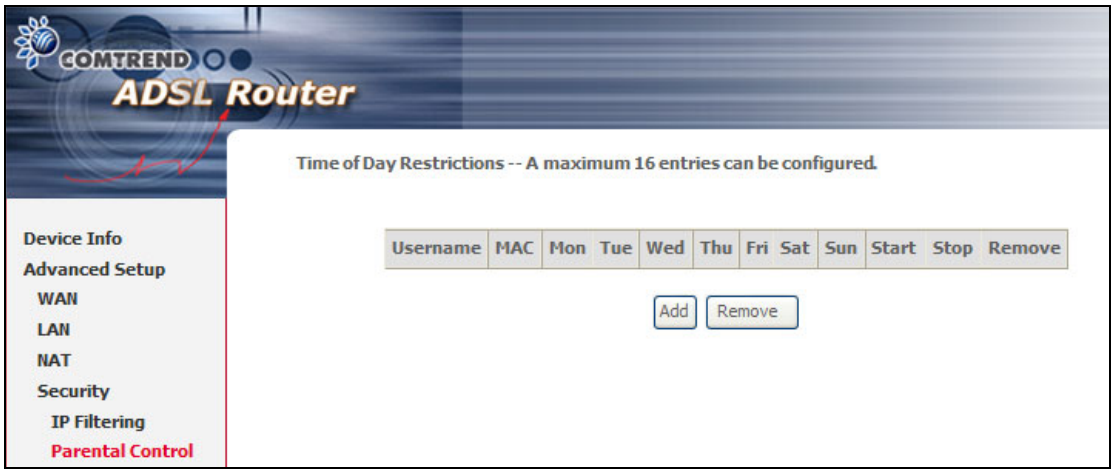
To add a filtering rule, click the **Add** button. The following screen will be displayed.



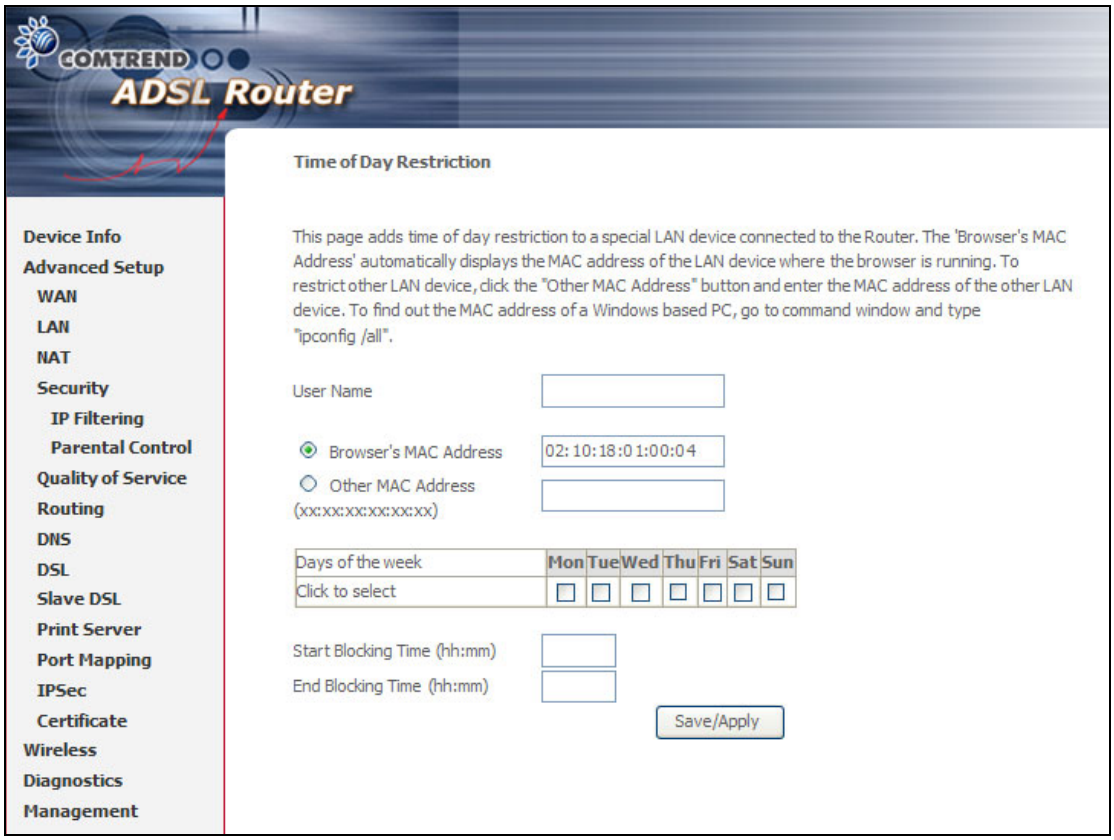
To configure the parameters, please reference **Outgoing** table above.

6.4.3 Parental Control

This allows parents, schools, and libraries to set access times for Internet use.



To add a parental control click the **Add** button and the following screen will display.



Username:	Name of the Filter.
MAC:	Displays MAC address of the LAN device on which the browser is running.
Mon, Tue, Wed, Thu, Fri, Sat, Sun:	Days when the restrictions are applied.
Start, Stop:	The time when restrictions start and stop.

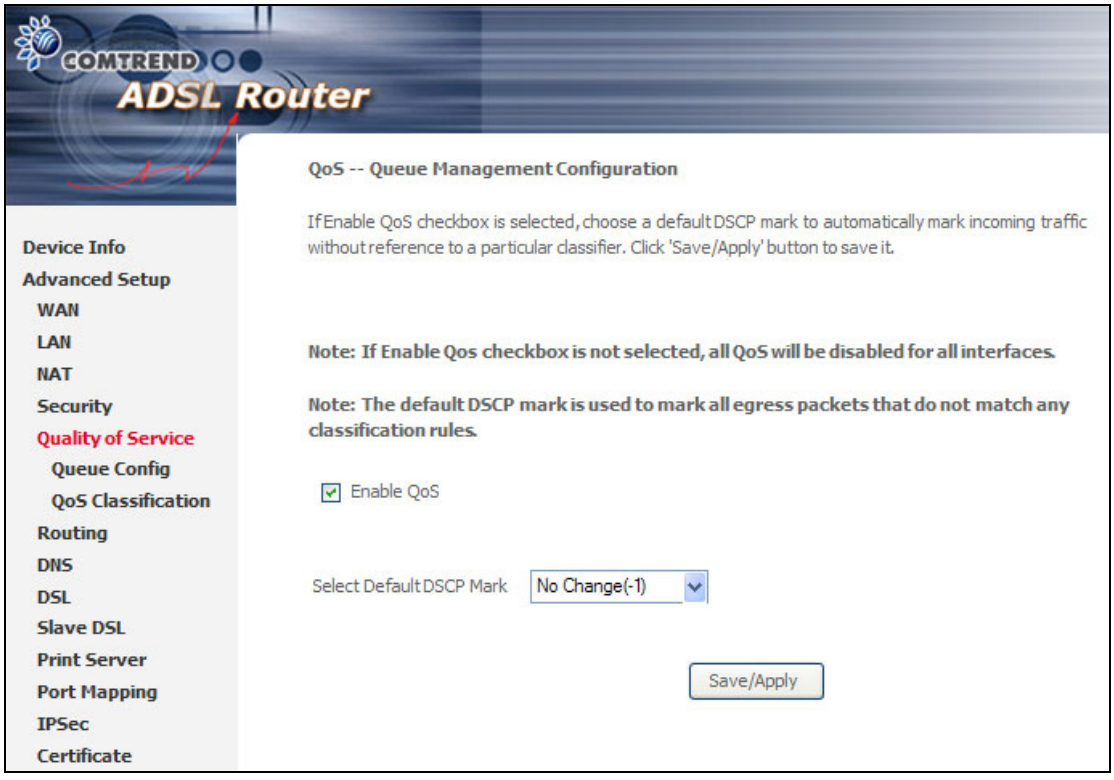
6.5 Quality of Service

NOTE: QoS is not yet supported for bonded routers. However, it is included here in the event that a future firmware upgrade supports this feature.

6.5.1 Queue Management Configuration

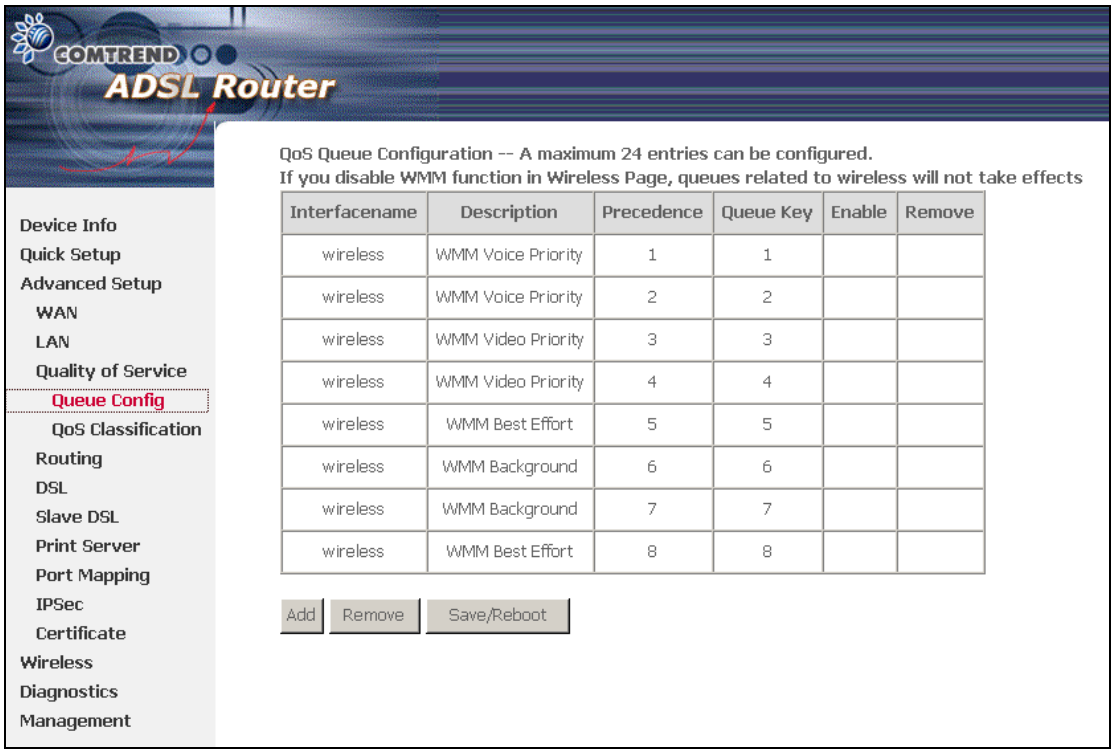
Quality of service: Quality of Service can provide different priority to different users or data flows, or guarantee a certain level of performance to a data flow in accordance with requests from Queue Prioritization.

Differentiated Services Code Point (DSCP): You can assign DSCP mark that specifies the per hop behavior for a given flow of packets in the Internet Protocol (IP) header.

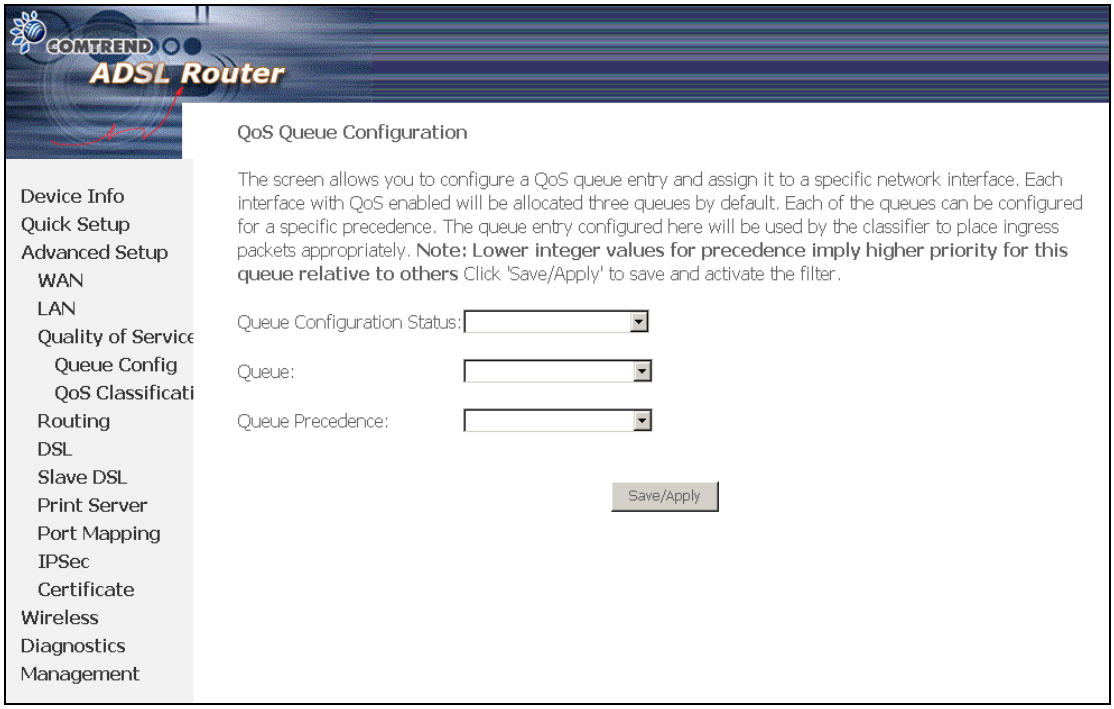


6.5.2 QoS Queue Configuration

This follows the "Differentiated Services" rule of IP QoS. You can create a new Queue rule by assigning interface, Enable/Disable and Precedence. This router uses various queuing strategies to tailor performance to requirements.



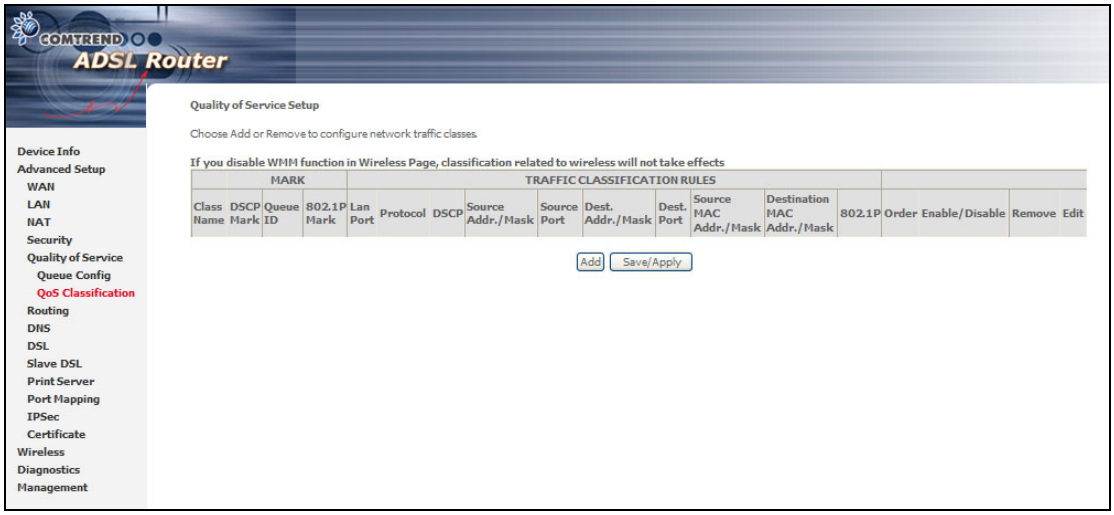
Click **Add** to display the following screen.



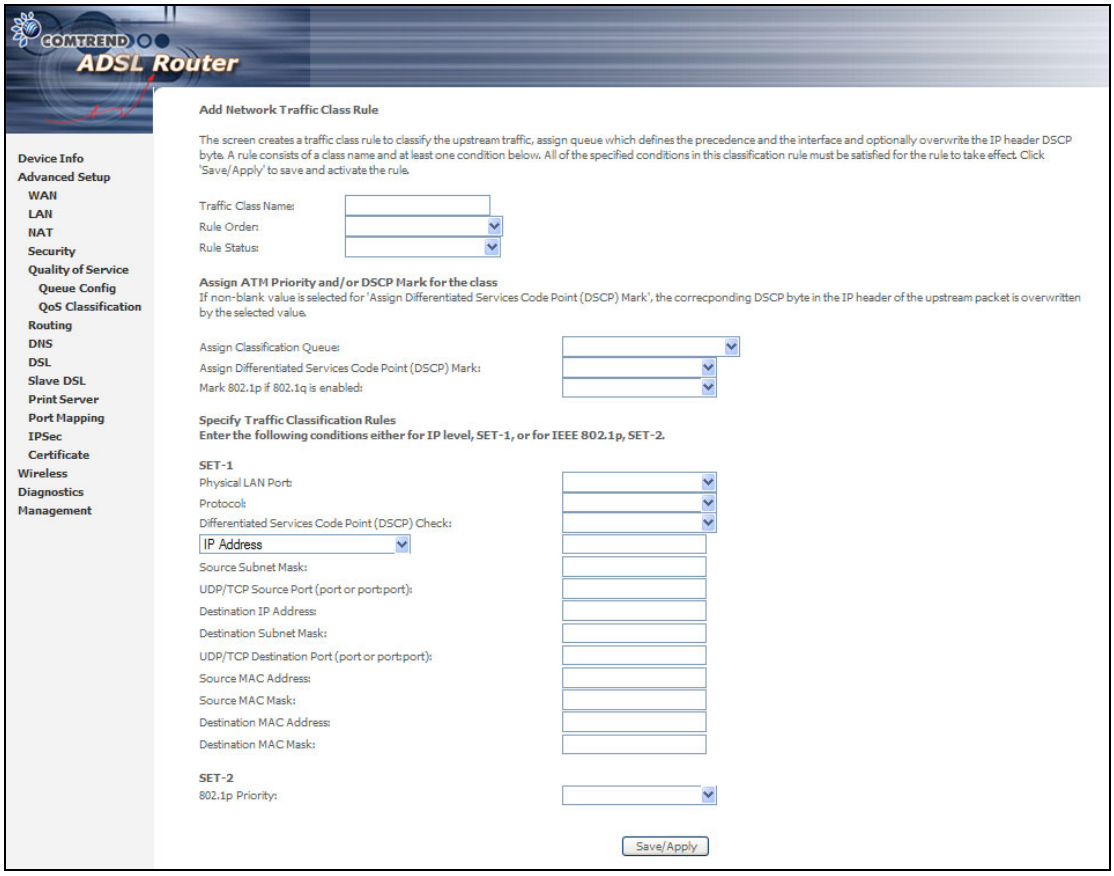
Queue Configuration Status: Make the queue Enable/Disable.

Queue: Assign queue to a specific network interface whose QoS is enabled.

Queue Precedence: Configure precedence for queue. Lower integer values for precedence imply higher priority for this queue relative to others.



Click **Add** to configure network traffic classes.



This screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.

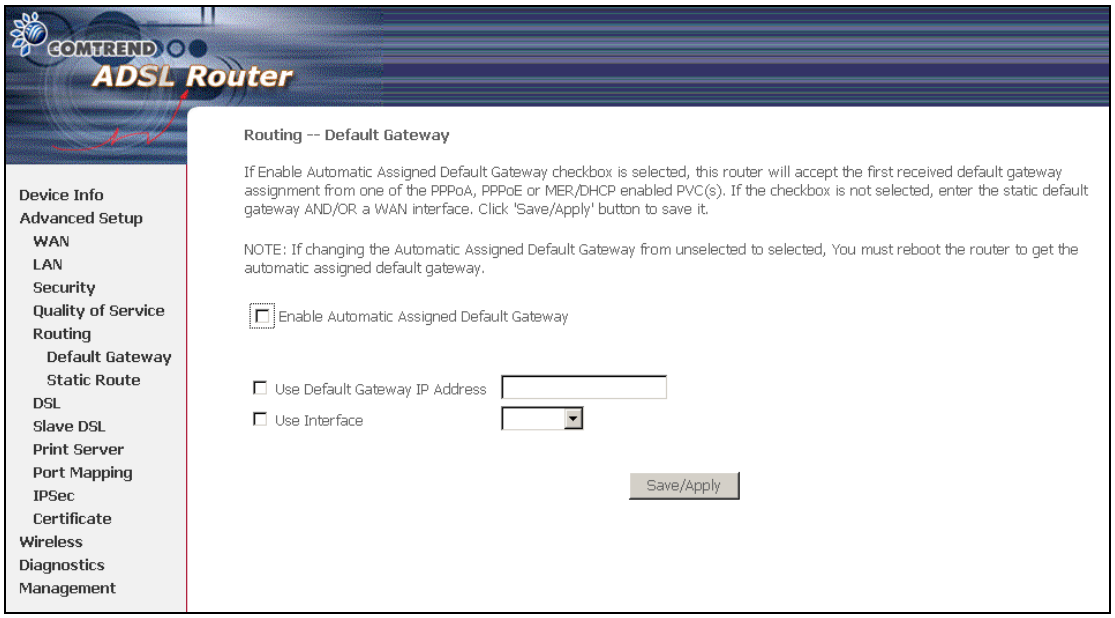
Click **Save/Apply** to save and activate the rule.

6.6 Routing

6.6.1 Default Gateway

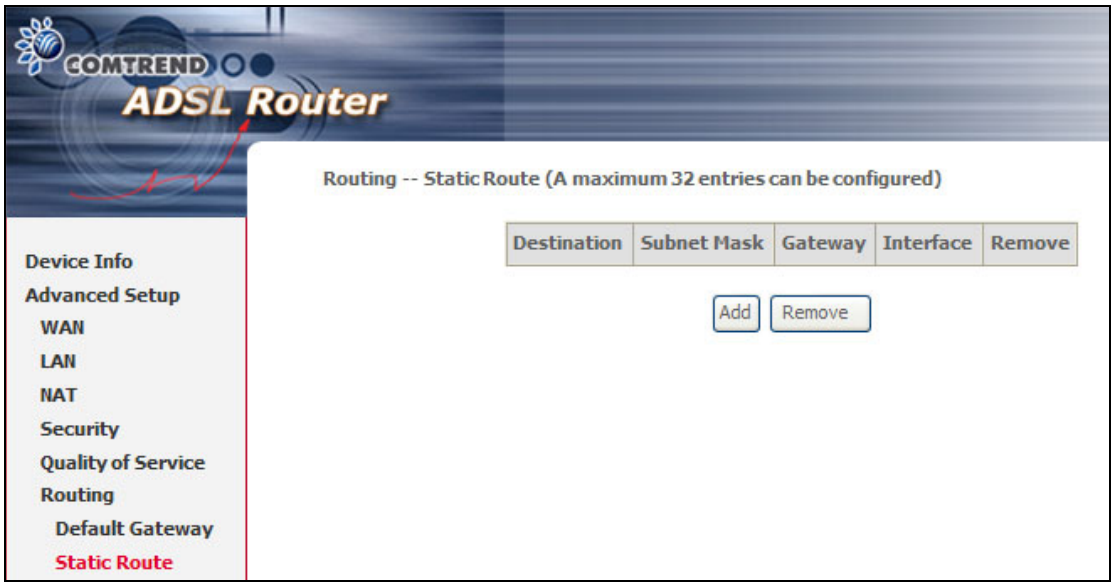
If the **Enable Automatic Assigned Default Gateway** checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER (DHCP enabled) PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR WAN interface. Click **Save/Apply.**

NOTE:	After enabling **Automatic Assigned Default Gateway**, you must reboot the router.

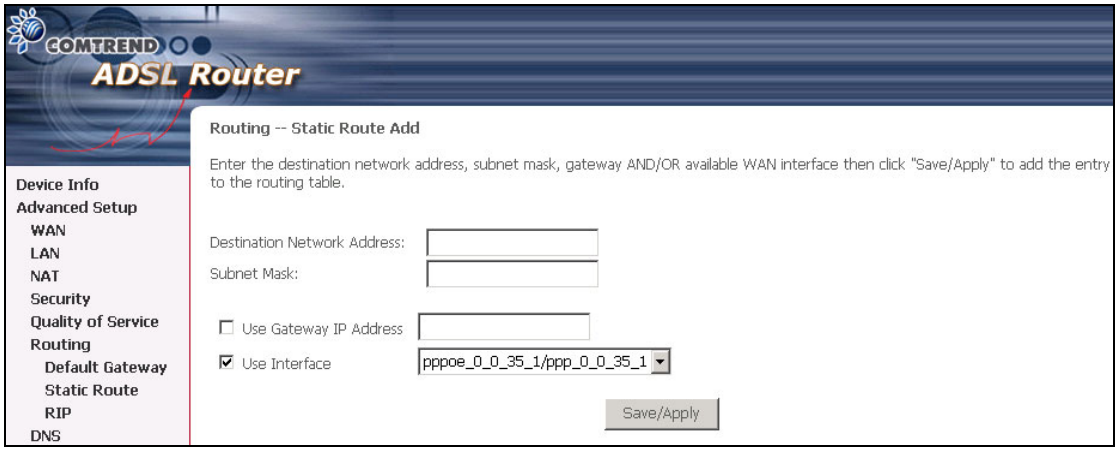


6.6.2 Static Route

Choose **Static Route** to display the Static Route screen. The Static Route screen lists the configured static routes, and allows configuring static routes. Choose **Add** or **Remove** to configure the static routes.



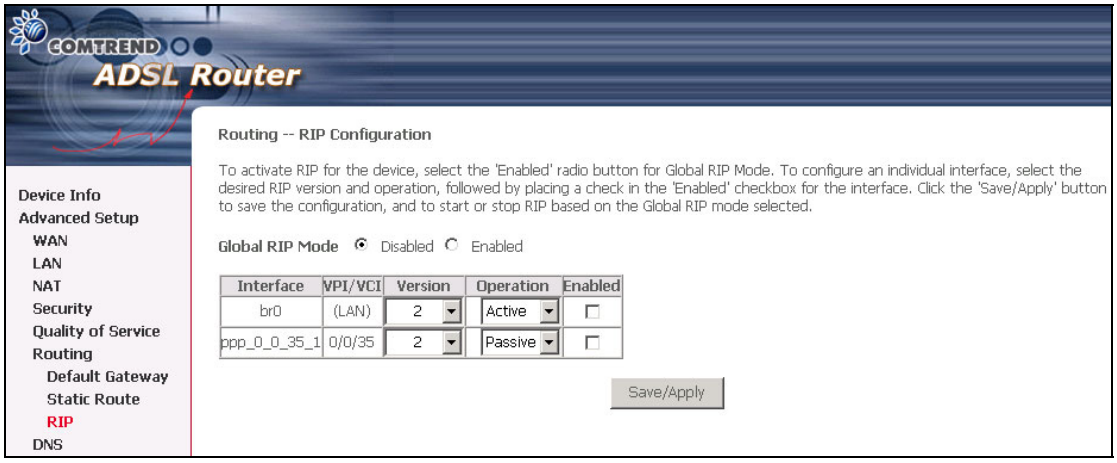
To add static route, click the **Add** button to display the following screen. Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click **Save/Apply** to add the entry to the routing table.



6.6.3 RIP

To activate RIP for the router, select the **Enabled** radio button for **Global RIP Mode**. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the **Enabled** checkbox for the interface.

Click **Save/Apply** to save the configuration and to start or stop RIP (based upon the Global RIP mode selected).

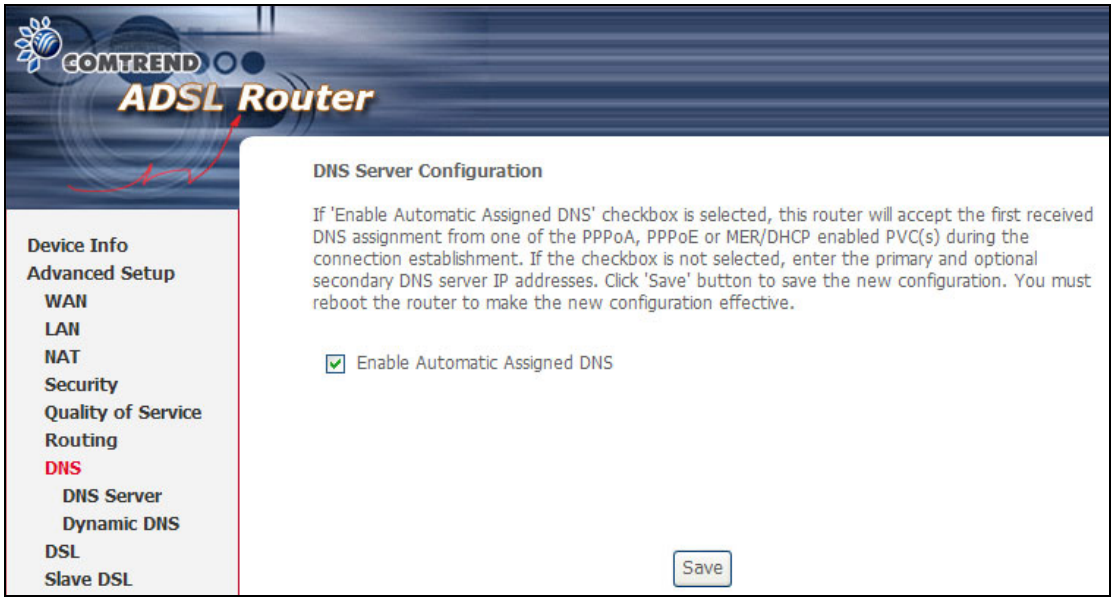


NOTE: This screenshot is based on PPPoE encapsulation.

6.7 DNS

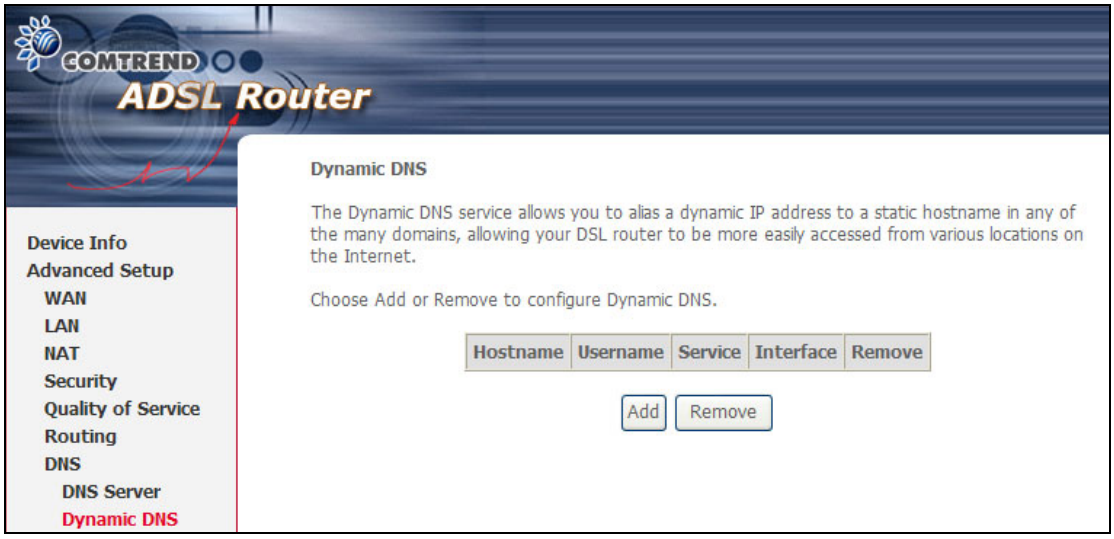
6.7.1 DNS Server

If **Enable Automatic Assigned DNS** checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER (DHCP enabled) PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click the **Save** button to save the new configuration. You must reboot the router to make the new configuration effective.



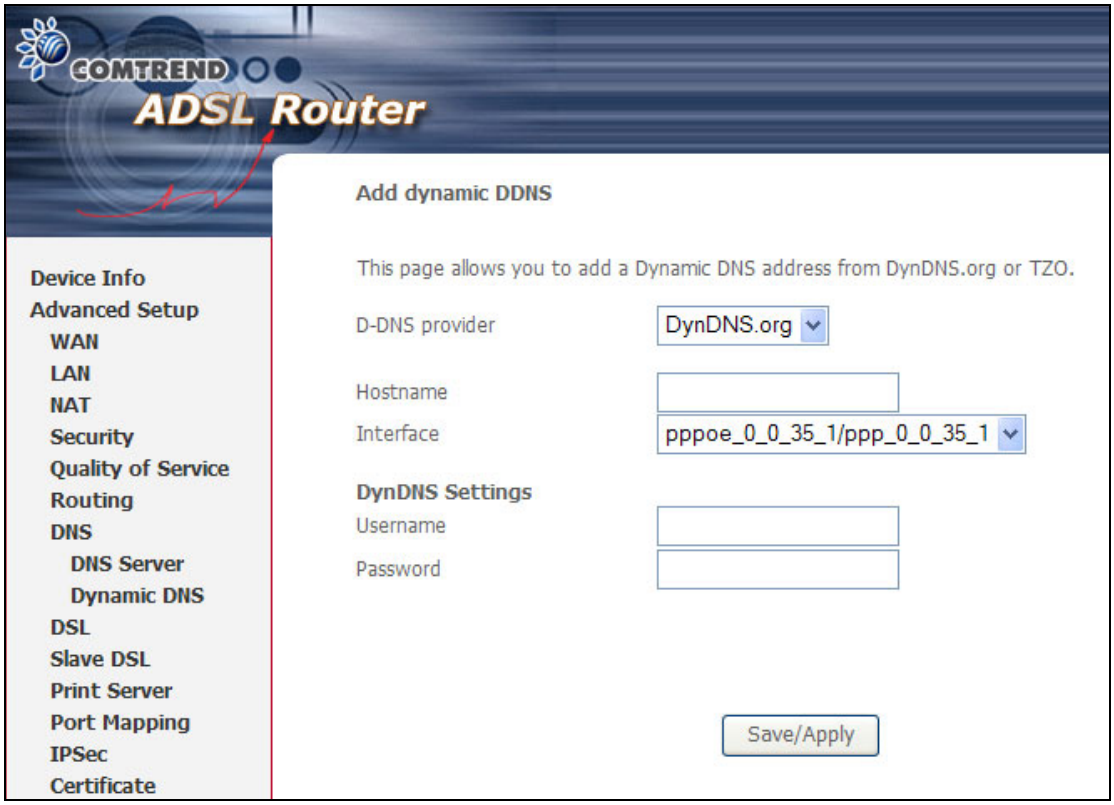
6.7.2 Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your ADSL router to be more easily accessed from various locations on the Internet.



NOTE:	The **Add** and **Remove** buttons will only be displayed if the CPE has already been assigned an IP address from the remote server.

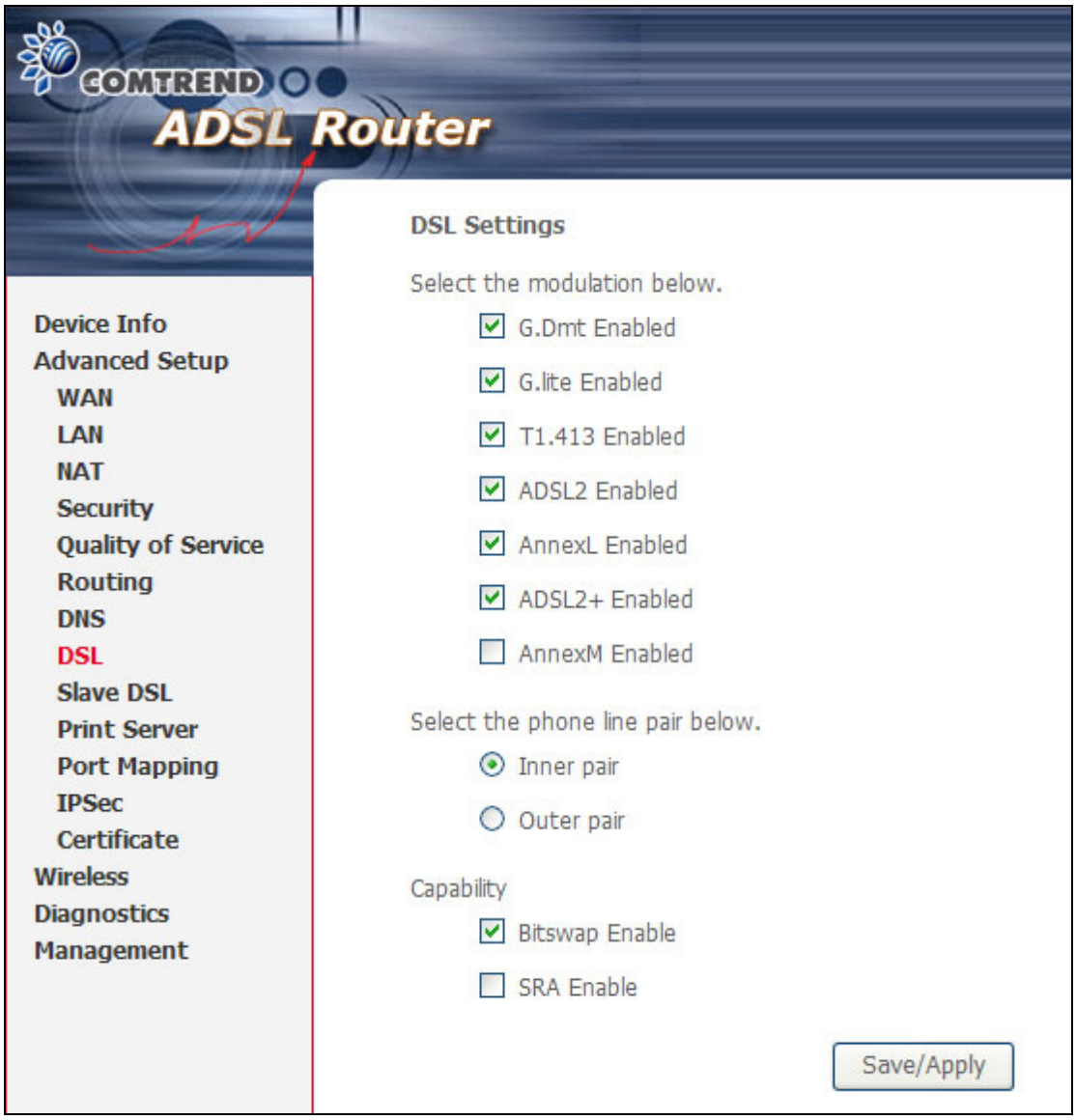
To add a dynamic DNS service, click **Add** and the following screen will be displayed:



D-DNS provider	Select a dynamic DNS provider from the list.
Hostname	Enter the name for the dynamic DNS server.
Interface	Select the interface from the list.
Username	Enter the username for the dynamic DNS server.
Password	Enter the password for the dynamic DNS server.

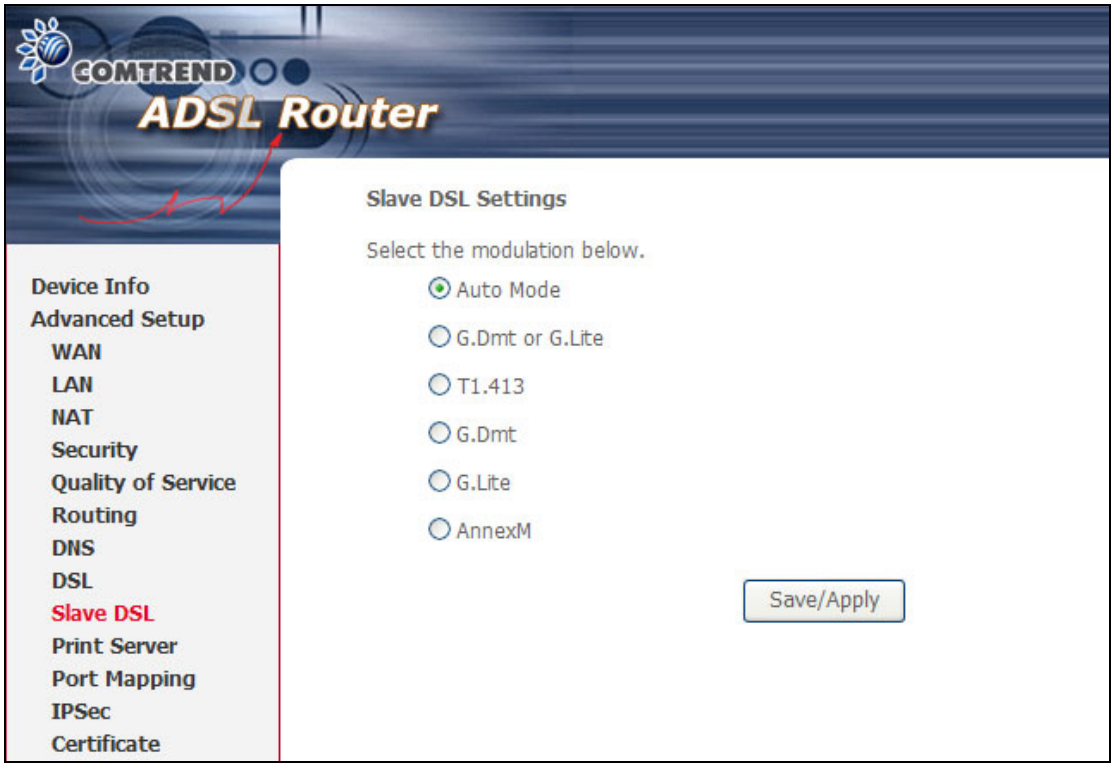
6.8 DSL / Slave DSL

To access the ADSL settings, first click On **Advanced Setup** and then click on **DSL**. This screen shows the settings available for **ADSL1**. For **ADSL2** use **Slave DSL**.



NOTE: Annex M is disabled by default for this router.

The **Slave DSL** settings screen is shown below.

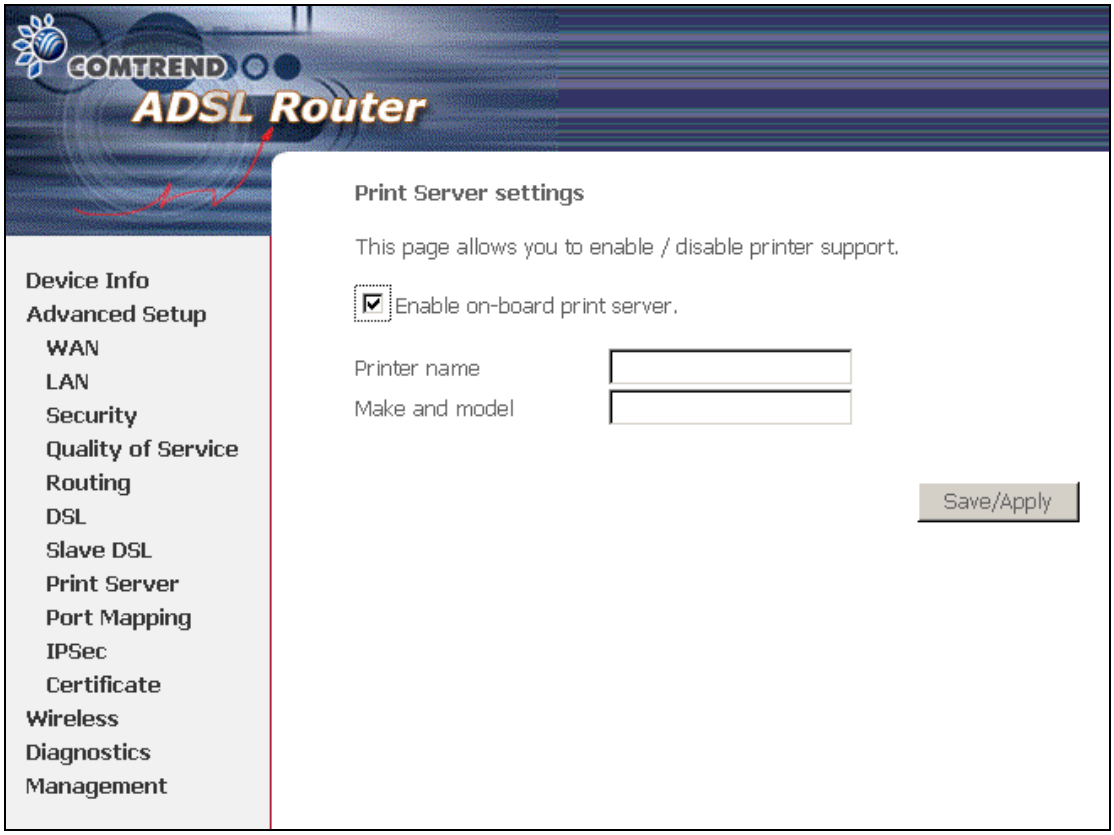


This table describes the DSL settings.

Option	**Description**
G.dmt	Sets G.Dmt if you want the system to use G.Dmt mode.
G.Lite	Sets G.Lite if you want the system to use G.Lite mode.
T1.413	Sets the T1.413 if you want the system to use T1.413 mode.
ADSL2	The router can support the functions of ADSL2.
AnnexL	The router can support/enhance the long loop test.
ADSL2+	The router can support the functions of ADSL2+.
AnnexM	Enables a higher "upstream" data rate, by making use of some downstream channels.
Inner Pair	Reserved only
Outer Pair	Reserved only
Bitswap Enable	Allows bitswapping function
SRA Enable	Allows seamless rate adaptation

6.9 Print Server

This router is equipped with one high-speed USB2.0 host connection. With software support, users can connect USB devices such as a printer and hard disc to the router. For this software release, only the printer server is supported.

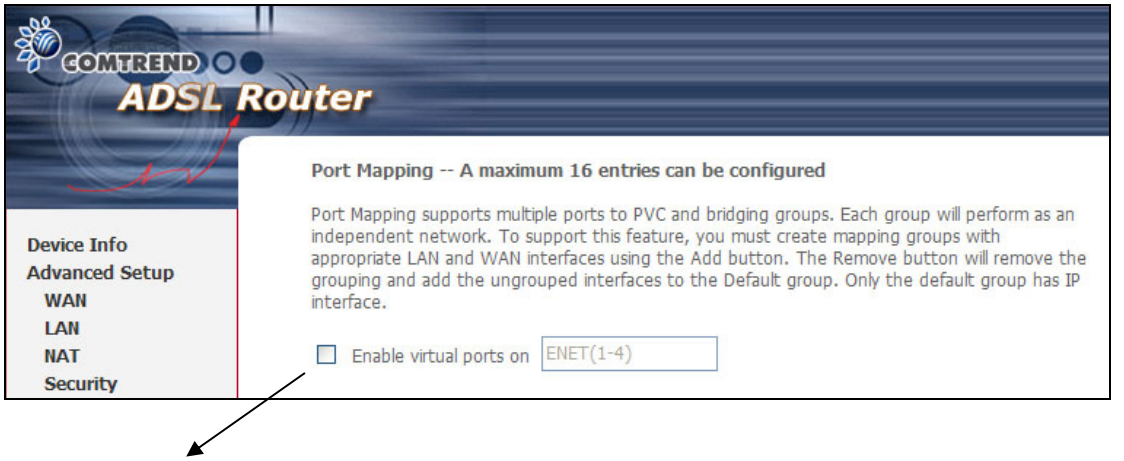


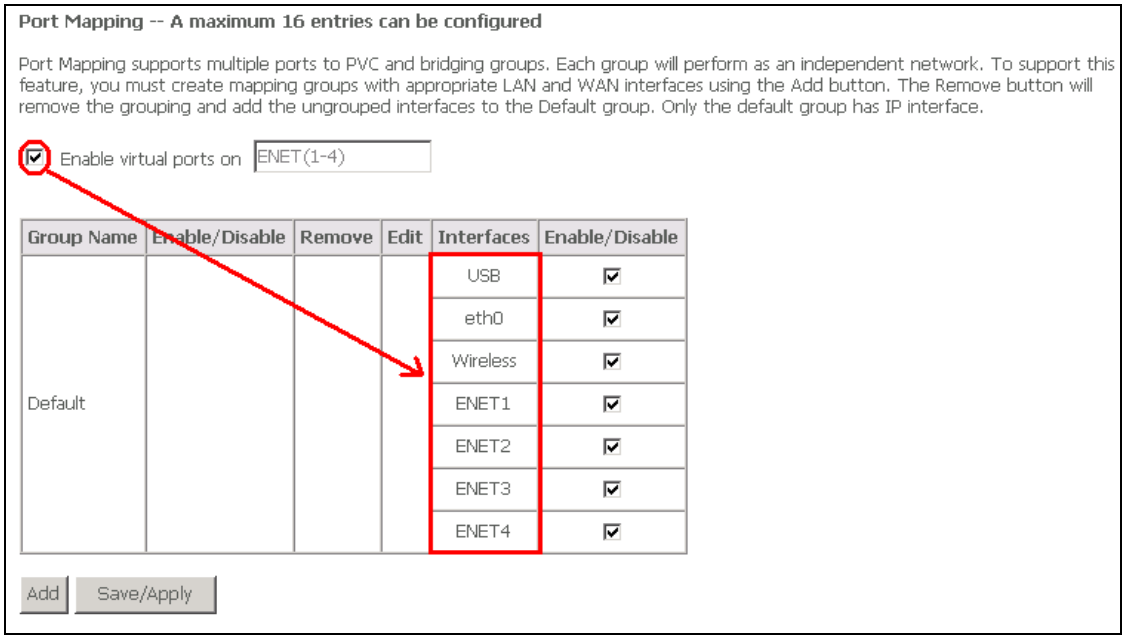
Please refer to Appendix B: Printer Server for detailed instructions.

6.10 Port Mapping

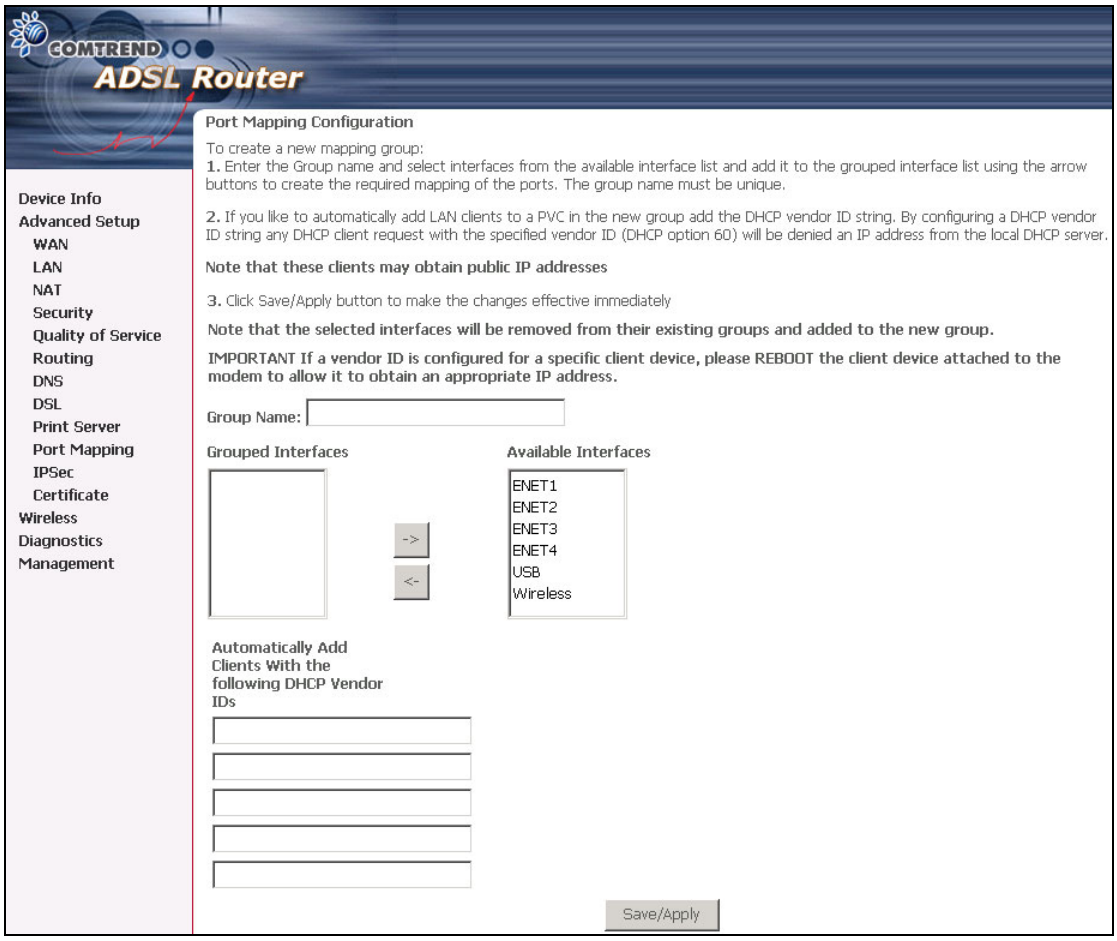
Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group.

As shown below, when you tick the Enable virtual ports on, all of the LAN interfaces will be grouped together as a default.





To add a port mapping group, click the **Add** button.



To create a group from the list, first enter the group name and then select from the available interfaces on the list.

Automatically Add Clients With the Following DHCP Vendor IDs:

Add support to automatically map LAN interfaces including Wireless and USB to PVC's using DHCP vendor ID (option 60). The local DHCP server will decline and send the requests to a remote DHCP server by mapping the appropriate LAN interface. This will be turned on when PortMapping is enabled.

There are 4 PVCs (0/33, 0/36, 0/37, 0/38). VPI/VCI=0/33 is for PPPoE and the others are for IP set-top box (video). The LAN interfaces are ENET1, ENET2, ENET3, ENET4, Wireless and USB.

Port mapping configuration are:

1. Default: ENET1, ENET2, ENET3, ENET4, Wireless and USB.
2. Video: nas_0_36, nas_0_37 and nas_0_38. The DHCP vendor ID is "Video".

The CPE deco server is running on "Default". And ISP's deco server is running on PVC 0/36. It is for set-top box use only.

On the LAN side, the PC can get IP address from CPE deco server and access the Internet via PPPoE (0/33).

If the set-top box was connected with interface "ENET1" and send a deco request with vendor id "Video", the CPE deco server would forward this request to ISP's deco server. Then the CPE will change the PortMapping configuration automatically. The PortMapping configuration would become:

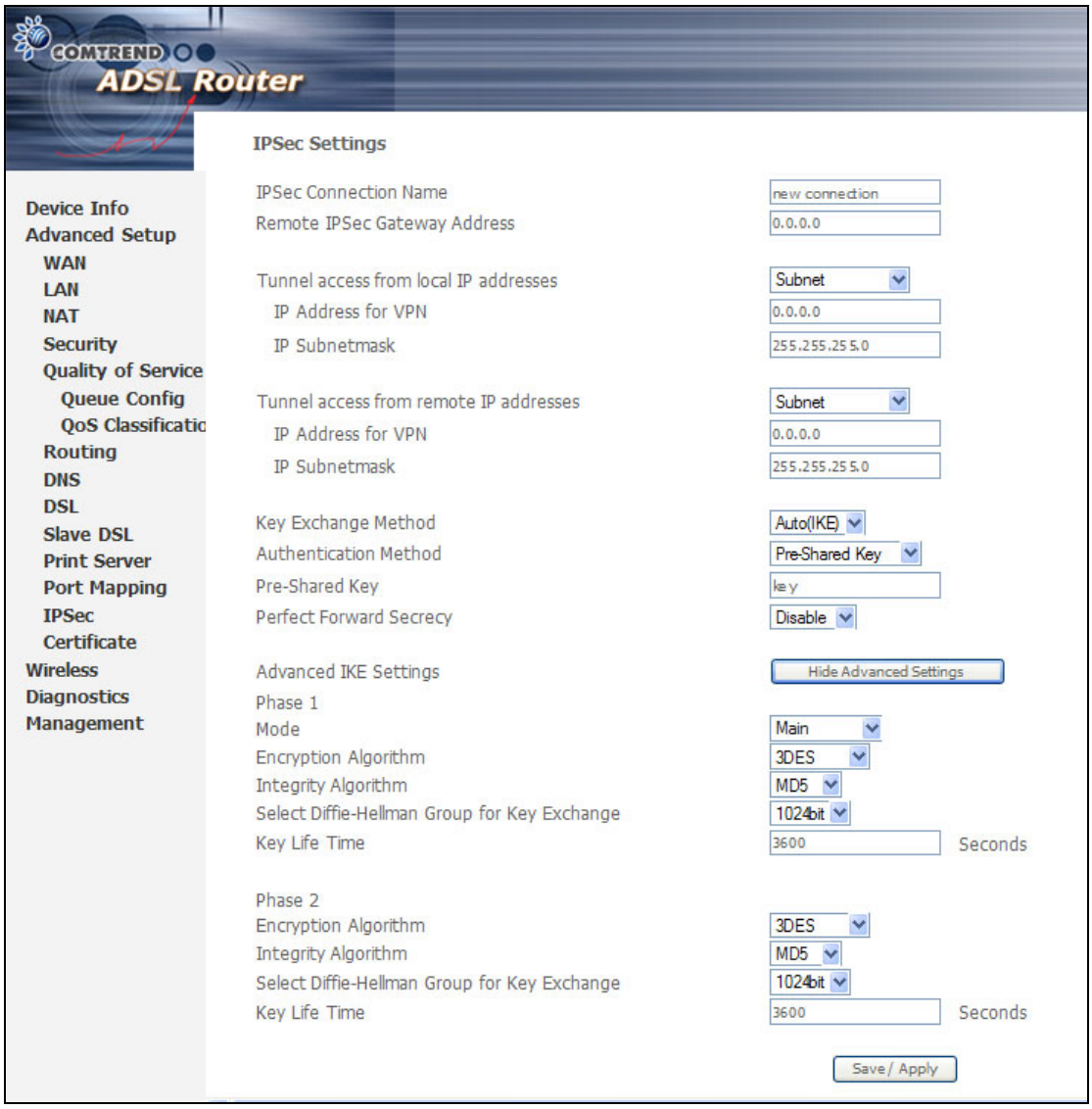
1. Default: ENET2, ENET3, ENET4, Wireless and USB.
2. Video: nas_0_36, nas_0_37, nas_0_38 and ENET1.

6.11 IPSec

You can add, edit or remove IPSec tunnel mode connections from this page.

By clicking **Add New Connection**, you can add a new IPSec termination rule.

In this case, the following screen will display.



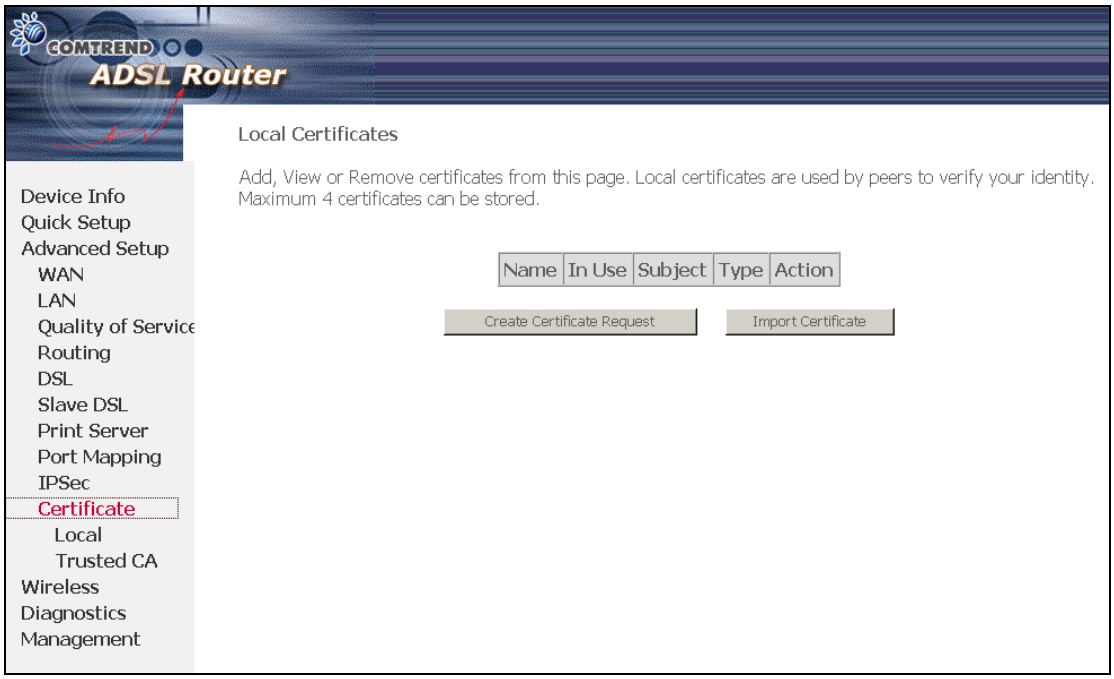
IPSec Connection Name	User-defined label
Remote IPSec Gateway Address (IP or Domain Name)	The IP address of remote tunnel Gateway, and you can use numeric address and domain name
Tunnel access from local IP addresses	It chooses methods that specify the acceptable host IP on the local side. It has single and subnet.
IP Address for VPN	If you choose “single”, please entry the host IP address for VPN. If you choose “subnet”, please entry the subnet information for VPN.
Tunnel access from remote IP addresses	It chooses methods that specify the acceptable host IP on the remote side. It has single and subnet.

IP Address for VPN	If you choose "single", please entry the host IP address for VPN. If you choose "subnet", please entry the subnet information for VPN.
Key Exchange Method	It has two modes. One is auto and the other is manual.
Authentication Method	It has either pre-shared key or x.509.
Pre-Shared Key	Input Pre-shared key
Perfect Forward Secrecy	Enable/disable the method that is Perfect Forward Secrecy.
Advanced IKE Settings	On IPSec Auto mode, you need to choose the setting of two phases. Click the button then choose which modes, Encryption Algorithm, Integrity Algorithm, Select Diffie-Hellman Group for Key Exchange, key time on different phases.

6.12 Certificate

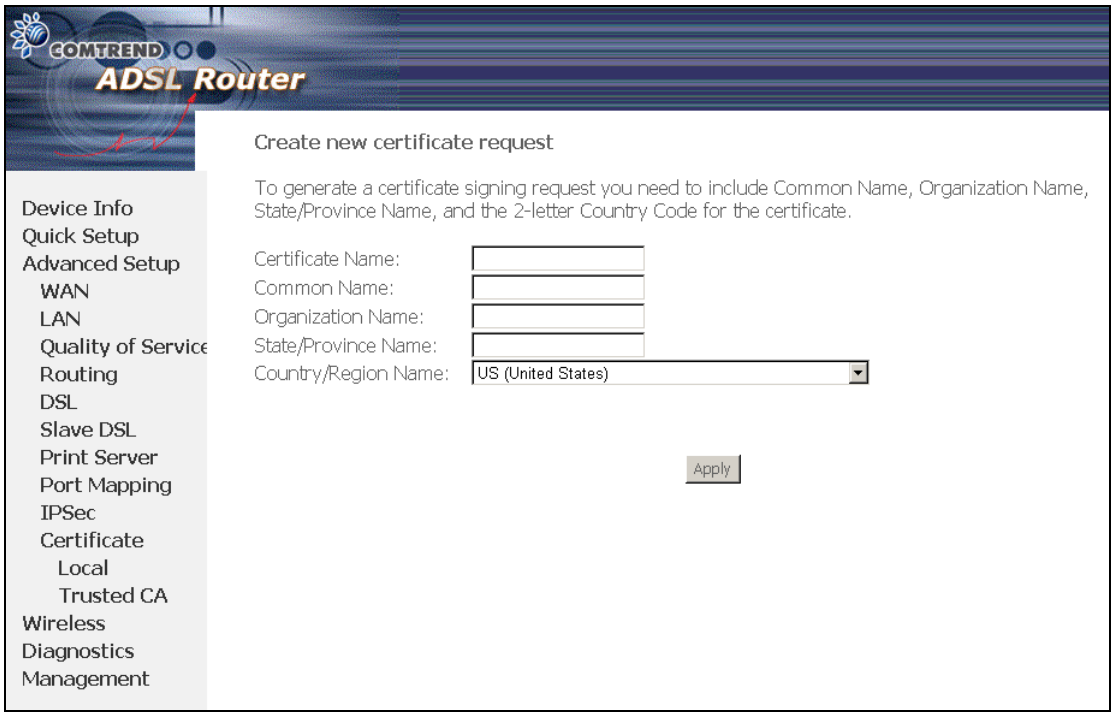
A certificate is a public key, attached with its owner's information (company name, server name, personal real name, contact e-mail, postal address, etc) and digital signatures. There will be one or more digital signatures attached on the certificate, indicating that these signers have verified that certificate is valid.

6.12.1 Local



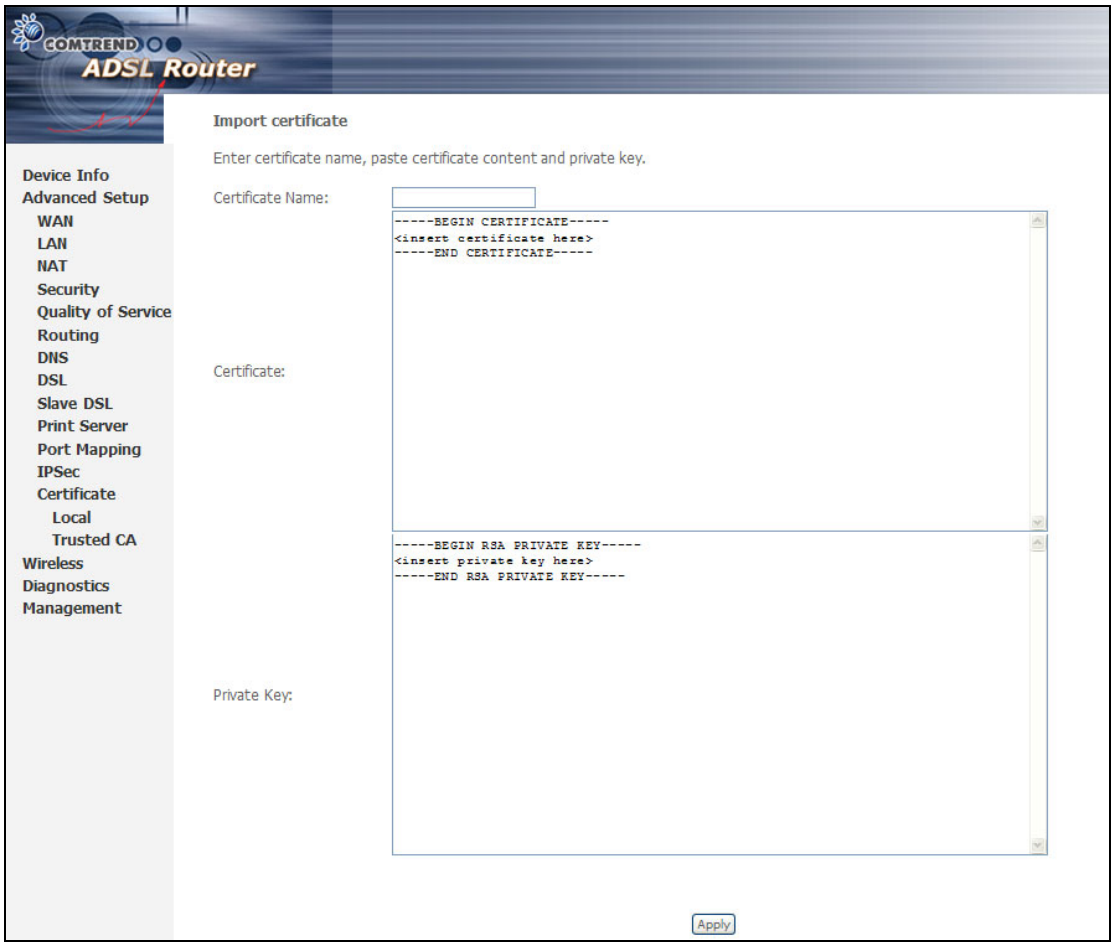
Click **Create Certificate Request** to generate a certificate signing request. The certificate signing request can be submitted to the vendor/ISP/ITSP to apply for a certificate. Some information must be included in the certificate signing request. Actually, your vendor/ISP/ITSP will ask you to provide the information they require and to provide the information in the format they regulate. The explanation for each column in the following table is only for reference.

Click **Apply** to generate a private key and a certificate signing request.



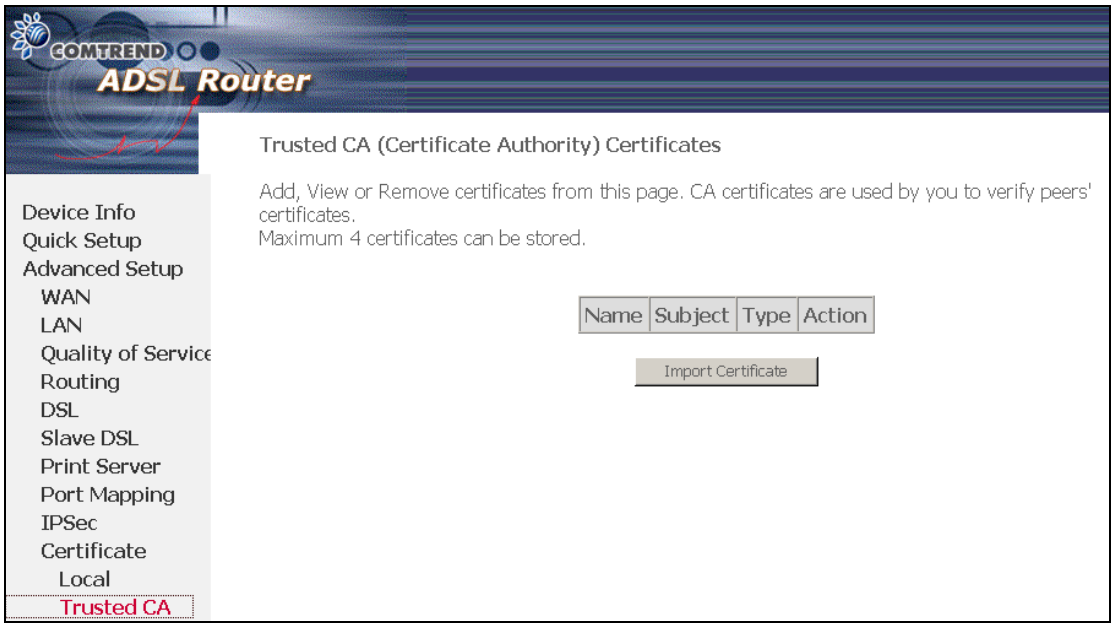
Certificate Name	A user-defined name for the certificate.
Common Name	Usually, it is the fully qualified domain name for the machine.
Organization Name	The exact legal name of your organization. Do not abbreviate.
State/Province Name	The state or province where your organization is located. It cannot be abbreviated.
Country/Region Name	The two-letter ISO abbreviation for your country.

The following screen is used to paste the certificate content and the private key provided by your vendor/ISP/ITSP.

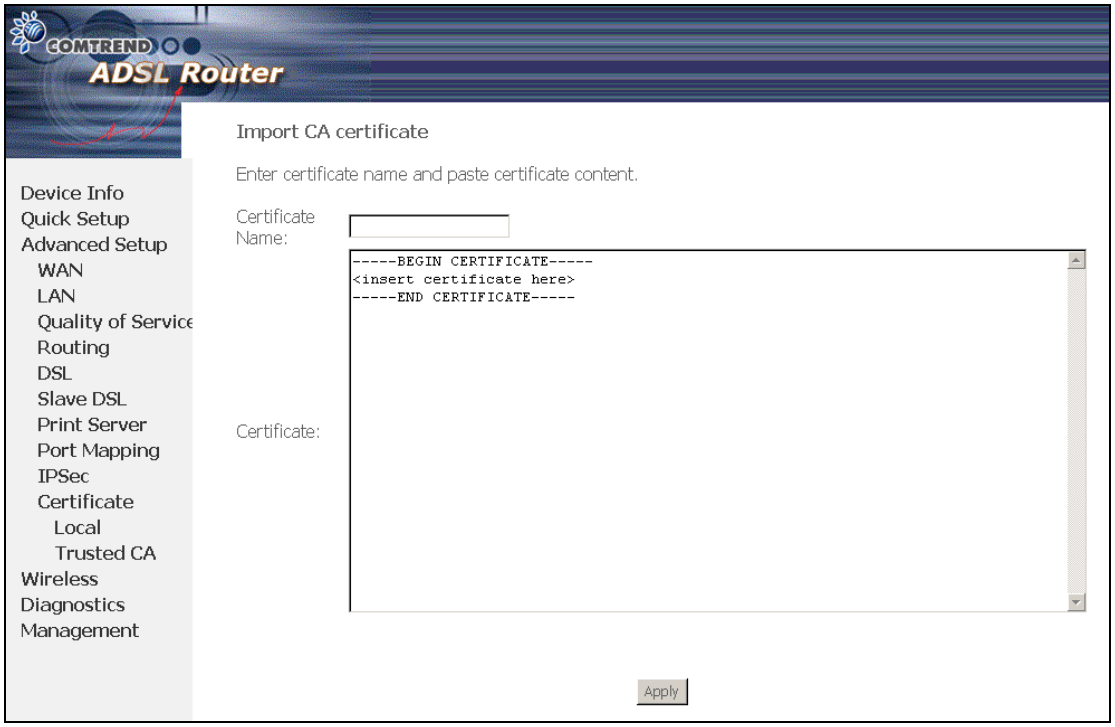


6.12.2 Trusted CA

CA is the abbreviation for Certificate Authority. CA is a part of the X.509 system. It is itself a certificate, attached with the owner information of this certificate authority. But its purpose is not to do encryption/decryption. Its purpose is to sign and issue certificates; in order to prove the owner information of that certificate is correct.



Click **Import Certificate** to paste the certificate content of your trusted CA. Generally speaking, the certificate content will be provided by your vendor/ISP/ITSP and is used to authenticate the Auto-Configuration Server (ACS) that the CPE will connect to.

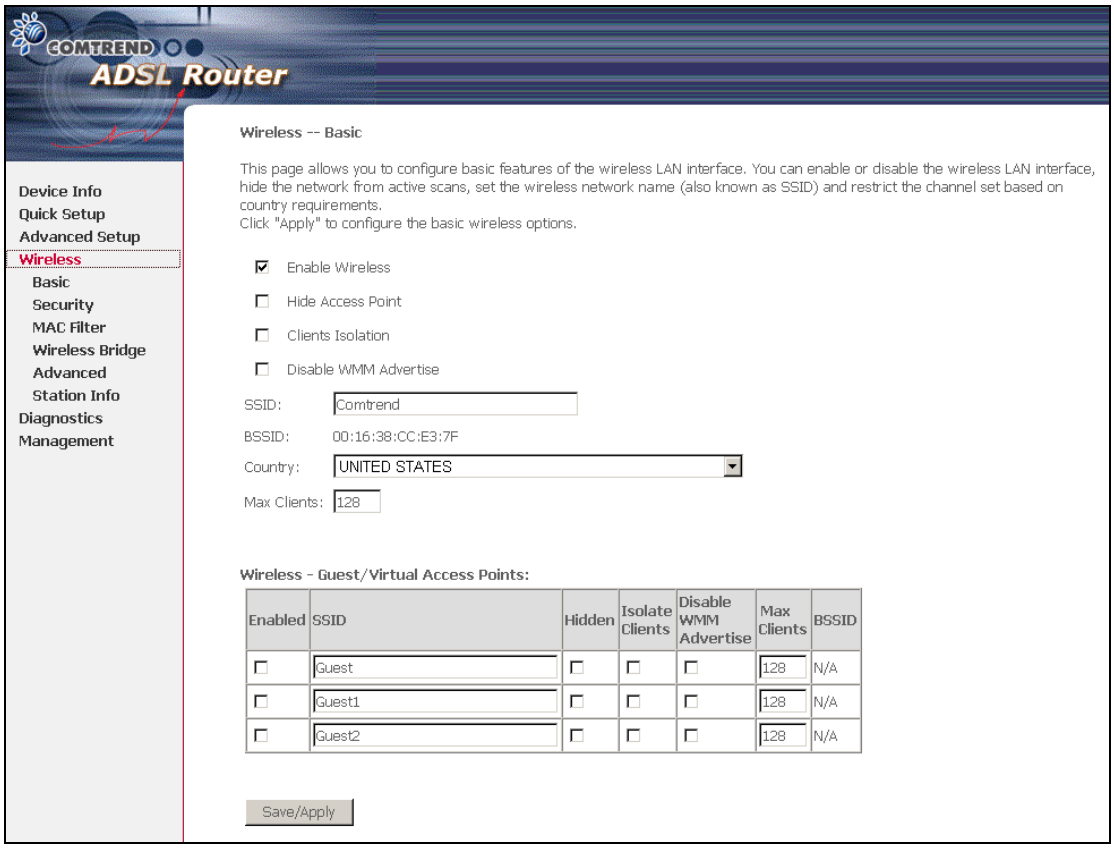


Chapter 7 Wireless

The Wireless dialog box allows you to enable the wireless capability, hide the access point, set the wireless network name and restrict the channel set.

7.1 Basic

The Basic option allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.



Click **Save/Apply** to configure the basic wireless options.

Option	Description
Enable Wireless	A checkbox that enables or disables the wireless LAN interface. When selected, the Web UI displays Hide Access point, SSID, and County settings. The default is Enable Wireless.
Hide Access Point	Select Hide Access Point to protect the access point from

	detection by wireless active scans. If you do not want the access point to be automatically detected by a wireless station, this checkbox should be de-selected. The station will not discover this access point. To connect a station to the available access points, the station must manually add this access point name in its wireless configuration. In Windows XP, go to the Network>Programs function to view all of the available access points. You can also use other software programs such as NetStumbler to view available access points.
Clients Isolation	1. Prevents clients PC from seeing one another in My Network Places or Network Neighborhood. 2. Prevents one wireless client communicating with another wireless client.
Disable WMM Advertise	Stops the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video). (wireless software version 3.10 and above)
SSID	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access. The naming conventions are: Minimum is one character and maximum number of characters: 32 bytes.
BSSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings. Each county listed in the menu enforces specific regulations limiting channel range: • US= worldwide • Japan=1-14 • Jordan= 10-13 • Israel= 1-13
Max Clients	The maximum number of clients that can access the router.

Wireless - Guest / Virtual Access Points	This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the radio buttons under the **Enable** heading. To hide a Guest SSID select its radio button under the **Hidden** heading. Do the same for **Isolate Client** and **Disable WMM Advertise** functions. For a description of these two functions, see the entries for "Client Isolation" and "Disable WMM Advertise" in this table. Similarly, for **Max Clients** and **BSSID** headings, consult the matching entries in this table. **NOTE:** Remote wireless hosts are unable to scan Guest SSIDs.

7.2 Security

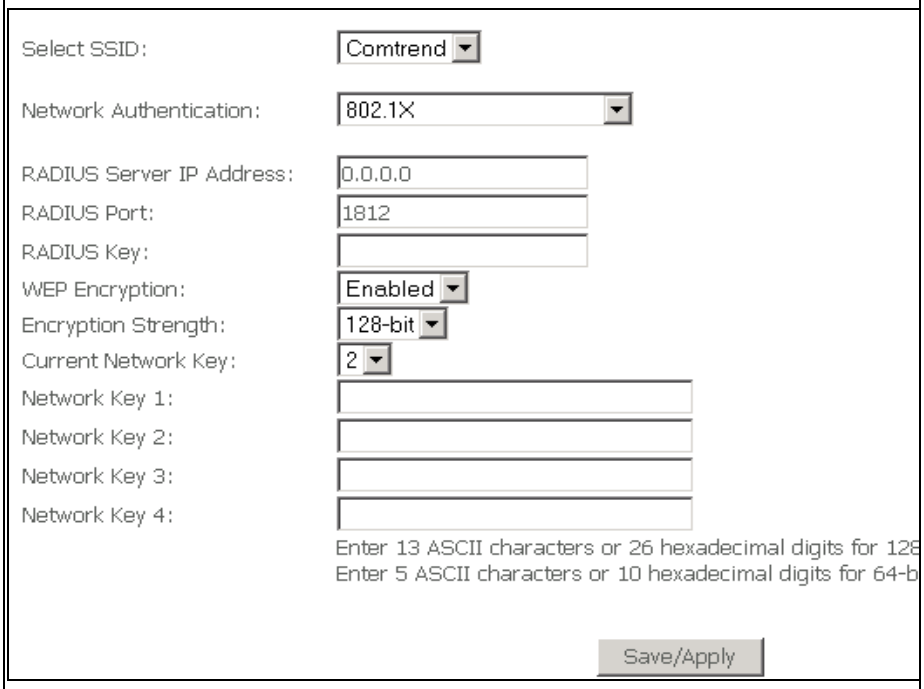
Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic. When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.

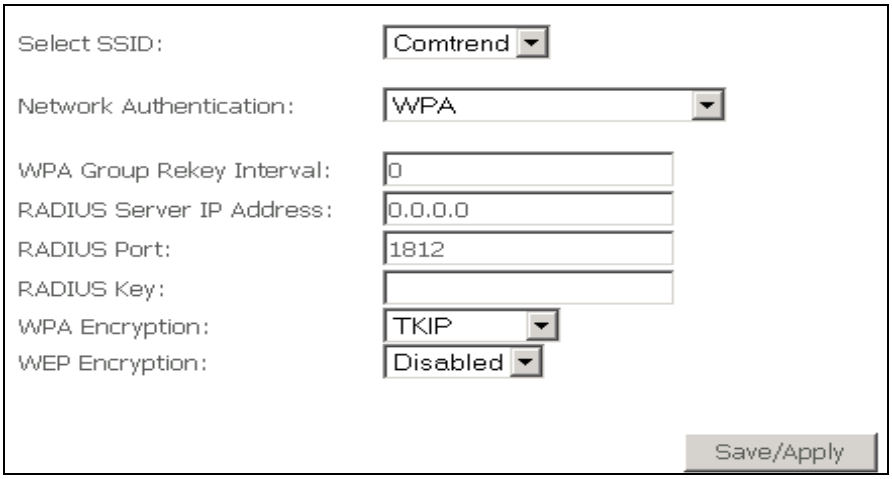
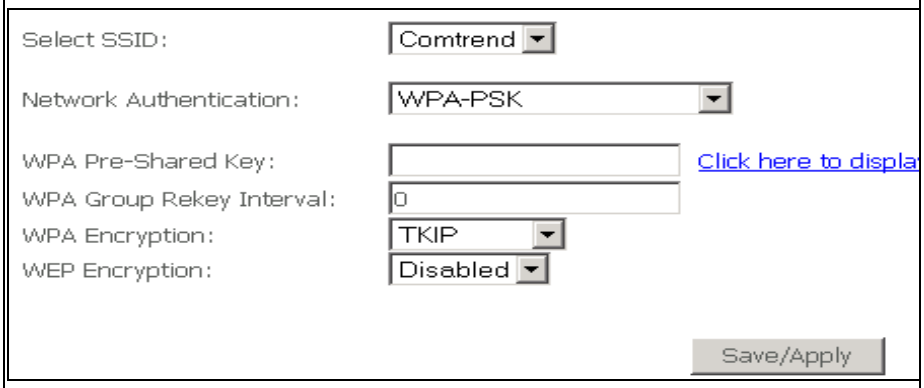
802.11 supports two subtypes of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The system that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then sends back a frame that indicates whether it recognizes the identity of the sending station.

Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from 802.11 wireless network communications channel.

The following screen appears when Security is selected. The Security page allows you to configure security features of the wireless LAN interface. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

Click **Apply** to configure the wireless security options.

Option	Description
Select SSID	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access. The naming conventions are: Minimum is one character and maximum number of characters: 32 bytes.
Network Authentication	It specifies the network authentication. When this checkbox is selected, it specifies that a network key be used for authentication to the wireless network. If the Network Authentication (Shared mode) checkbox is not shared (that is, if open system authentication is used), no authentication is provided. Open system authentication only performs identity verifications. Different authentication type pops up different settings requests. Choosing **802.1X**, enter RADIUS Server IP address, RADIUS Port, and RADIUS key. Also, enable WEP Encryption and the Encryption Strength.  Select the Current Network Key and enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys and enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

	Choosing **WPA**, you must enter WPA Group Rekey Interval.  Choosing **WPA-PSK**, you must enter WPA Pre-Shared Key and Group Rekey Interval. 
WEP Encryption	It specifies that a network key is used to encrypt the data is sent over the network. When this checkbox is selected, it enables data encryption and prompts the Encryption Strength drop-down menu. Data Encryption (WEP Enabled) and Network Authentication use the same key.
Encryption strength	A session's key strength is proportional to the number of binary bits comprising the session key file. This means that session keys with a greater number of bits have a greater degree of security, and are considerably more difficult to forcibly decode. This drop-down menu sets either a 64 8-bit (5-ASCII character or 10-hexadecimal character) or 128 8-bit (13-ASCII character or 26-hexadecimal character) key. If you set a minimum 128-bit key strength, users attempting to establish a secure communications channel with your server must use a browser capable of communicating with a 128-bit session key. The Encryption Strength settings do not display unless the network Authentication (shared Mode) check box is selected.

7.3 MAC Filter

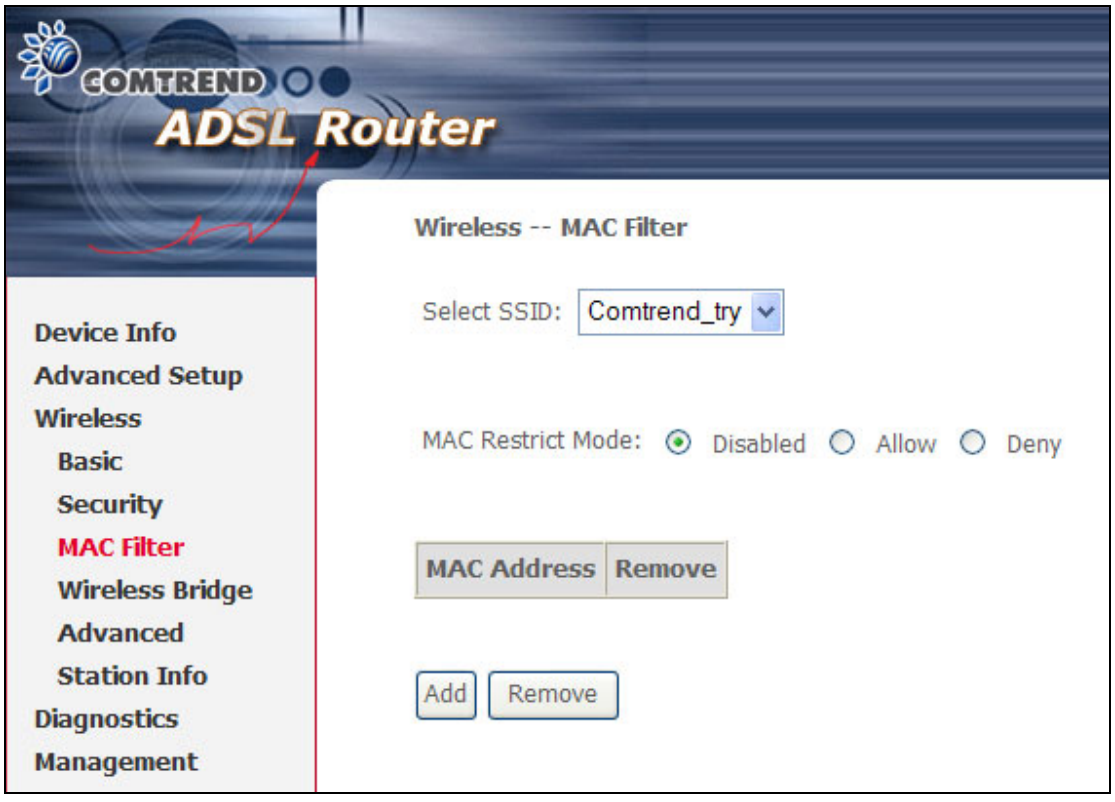
This MAC Filter page allows access to be restricted/allowed based on a MAC address. All NICs have a unique 48-bit MAC address burned into the ROM chip on the card. When MAC address filtering is enabled, you are restricting the NICs that are allowed to connect to your access point. Therefore, an access point will grant access to any computer that is using a NIC whose MAC address is on its "allows" list.

WiFi devices and access points that support MAC filtering let you specify a list of MAC addresses that may connect to the access point, and thus dictate what devices are authorized to access the wireless network. When a device is using MAC filtering, any address not explicitly defined will be denied access.

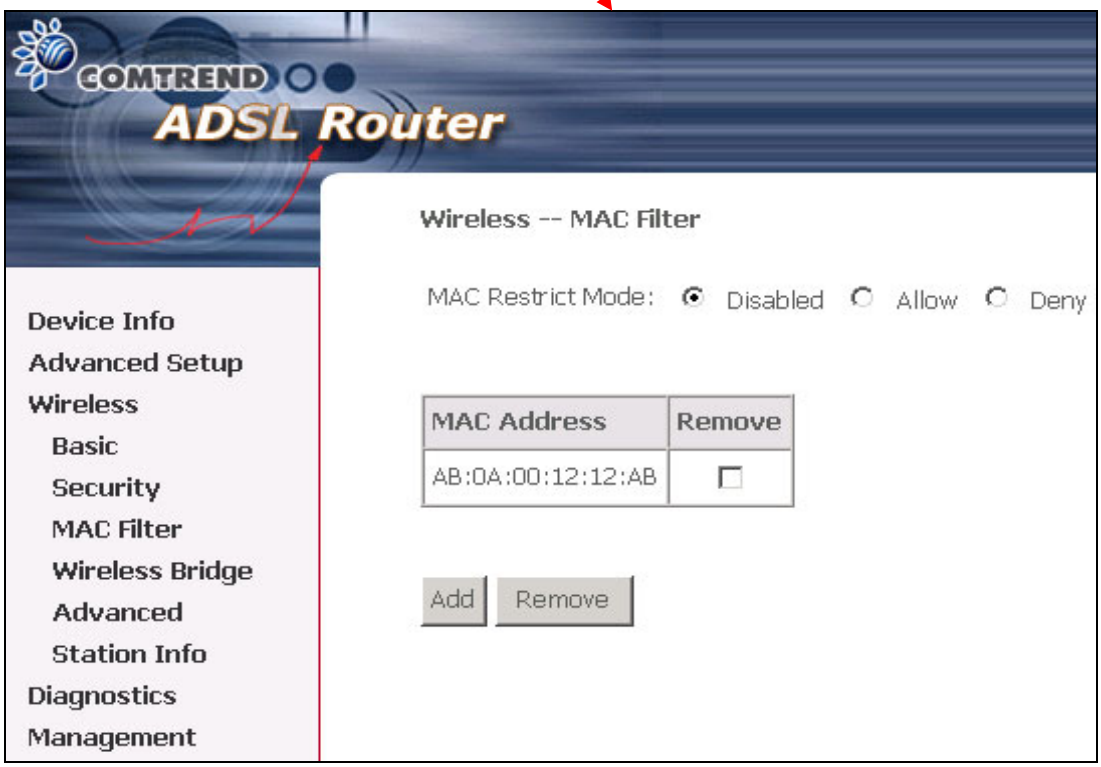
MAC Restrict mode: **Off**- disables MAC filtering; **Allow** – permits **access** for the specified MAC address; **deny**; reject access of the specified MAC address, then click the **SET** button.

To delete an entry**,** select the entry at the bottom of the screen and then click the **Remove** button, located on the right hand side of the screen.

To add a MAC entry, click **Add** and enter MAC address



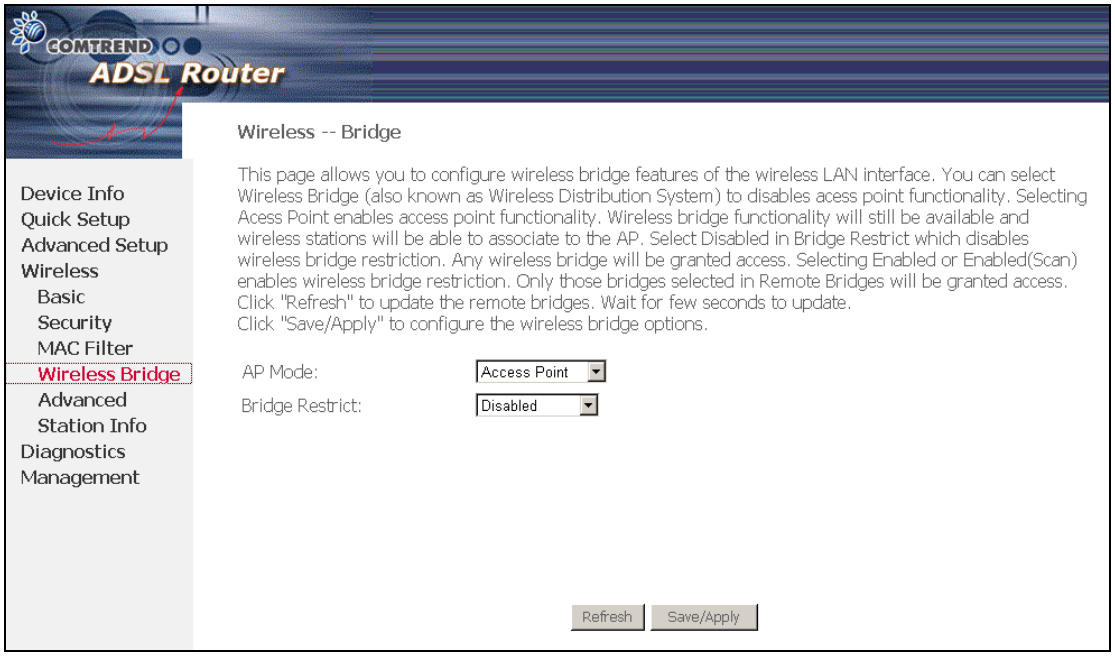
After choosing the Add button, the following screen appears. Enter the MAC address and click **Apply** to add the MAC address to the wireless MAC address filters.



Option	Description
MAC Restrict Mode	Radio buttons that allow settings of; Off: MAC filtering function is disabled. Allow: Permits PCs with listed MAC addresses to connect to access point. Deny: Prevents PCs with listed MAC from connecting to the access point.
MAC Address	Lists the MAC addresses subject to the Off, Allow, or Deny instruction. The Add button prompts an entry field that requires you type in a MAC address in a two-character, 6-byte convention: xx:xx:xx:xx:xx:xx where xx are hexadecimal numbers. The maximum number of MAC addresses that can be added is 60.

7.4 Wireless Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict, which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled (Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

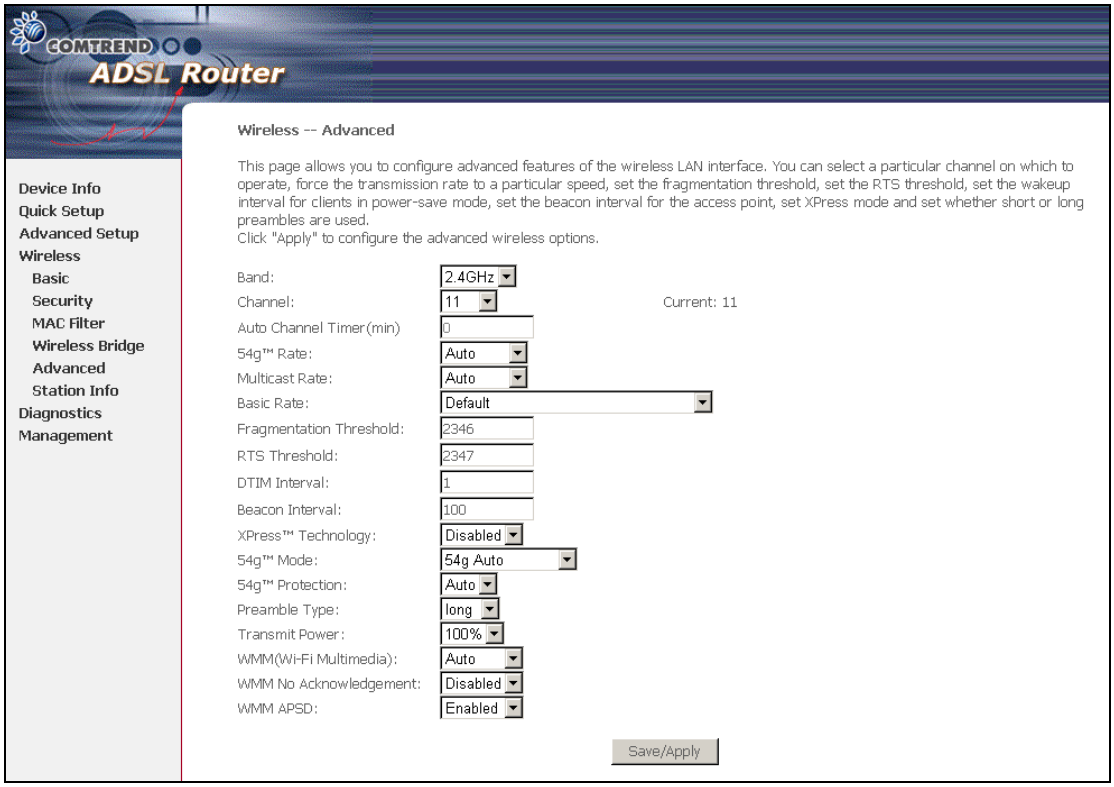


Feature	Options
AP Mode	Access Point Wireless Bridge
Bridge Restrict	Enabled Enabled (Scan) Disabled

7.5 Advanced

The Advanced page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

Click **Apply** to configure the advanced wireless options.



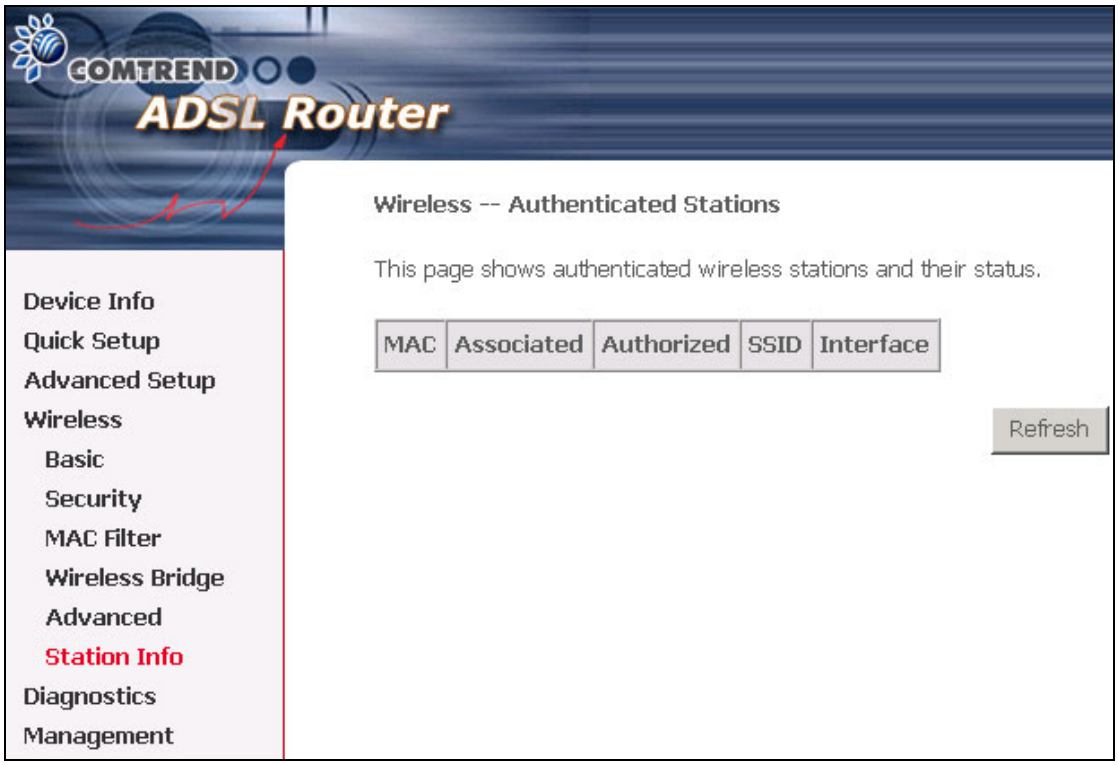
Option	Description
Band	The new amendment allows IEEE 802.11g units to fall back to speeds of 11 Mbps, so IEEE 802.11b and IEEE 802.11g devices can coexist in the same network. The two standards apply to the 2.4 GHz frequency band. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Channel	Drop-down menu that allows selection of a specific channel.
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)
54g Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Multicast Rate	Setting multicast packet transmit rate.
Basic Rate	Setting basic transmit rate.

Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM), also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions. Each beacon transmission identifies the presence of an access point. By default, radio NICs passively scan all RF channels and listen for beacons coming from access points to find a suitable access point. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point). The entered value is represented in ms. Default is 100. Acceptable entry range is 1 to 0xffff (65535)

Xpress ™ Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.
54g ™ Mode	Set the mode to 54g Auto for the widest compatibility. Select the mode to 54g Performance for the fastest performance among 54g certified equipment. Set the mode to 54g LRS if you are experiencing difficulty with legacy 802.11b equipment.
54g Protection	In Auto mode the router will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.
Preamble Type	Short preamble is intended for application where maximum throughput is desired but it doesn't cooperate with the legacy. Long preamble interoperates with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999
Transmit Power	The router will set different power output (by percentage) according to this selection.
WMM (Wi-Fi Multimedia)	The technology maintains the priority of audio, video and voice applications in a Wi-Fi network. It allows multimedia service get higher priority.
WMM No Acknowledge-ment	Refers to the acknowledge policy used at the MAC level. Enabling no Acknowledgement can result in more efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment.
WMM APSD	This is Automatic Power Save Delivery. It saves power.

7.6 Station Info

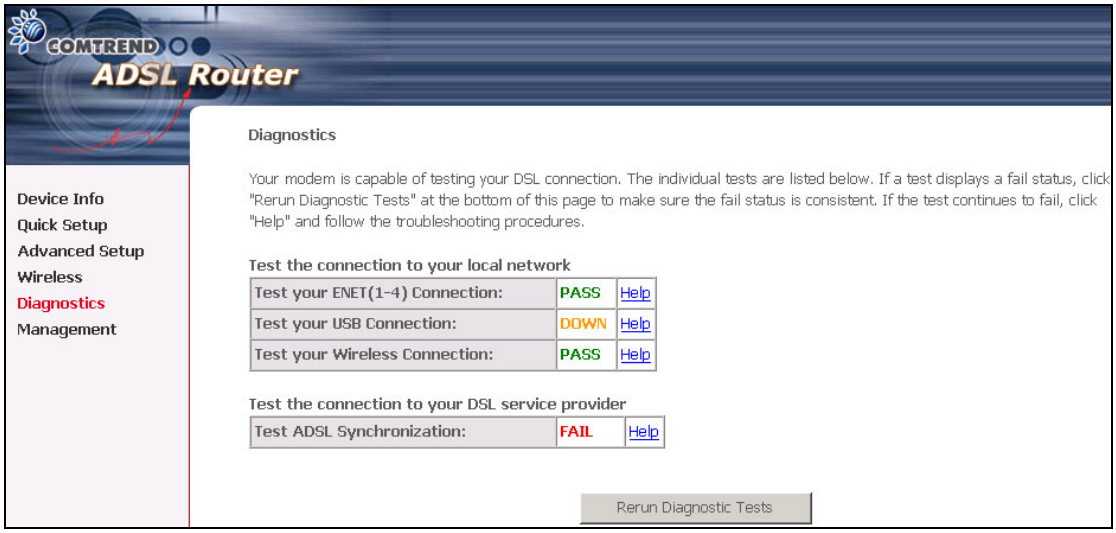
This page shows authenticated wireless stations and their status.



MAC	Lists the MAC address of all the stations.
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized	Lists those devices with authorized access.
SSID	Lists which SSID of the modem that the stations connect to.
Interface	Lists which interface of the modem that the stations connect to.

Chapter 8 Diagnostics

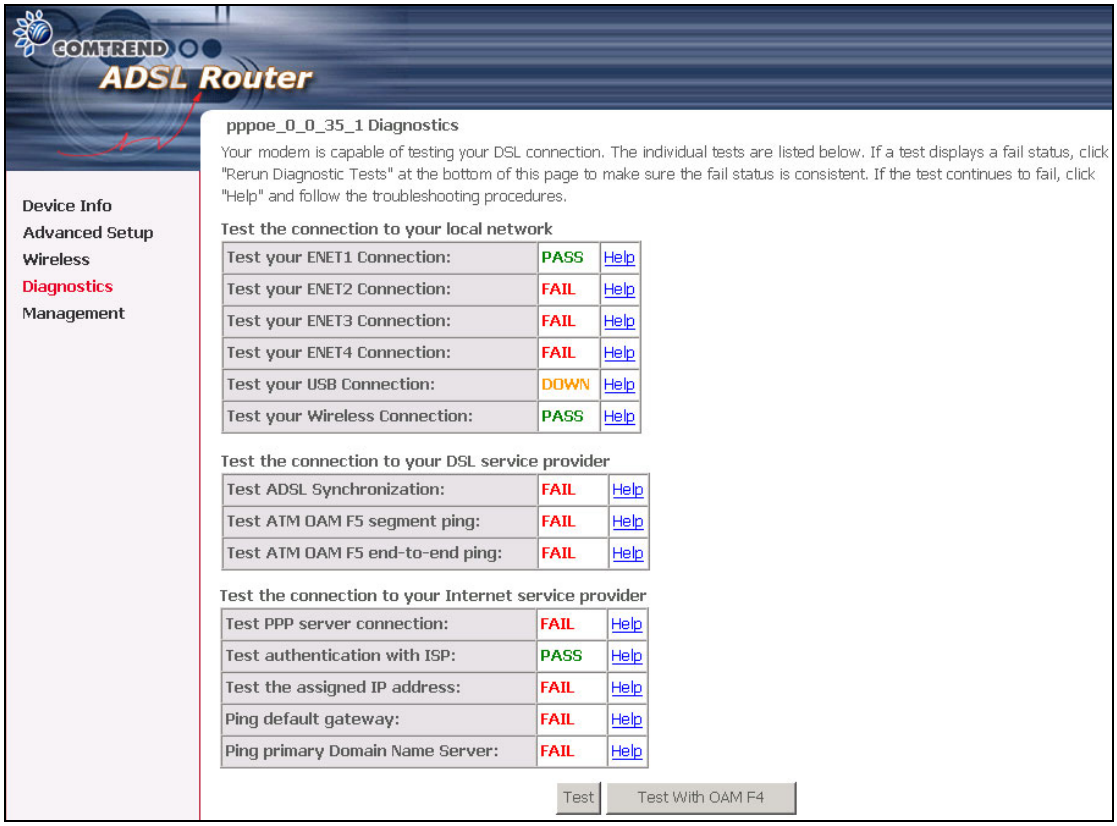
The Diagnostics menu provides feedback on the connection status of the router and the ADSL link. The individual tests are listed below. If a test displays a fail status, click **Rerun Diagnostic Tests** at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click **Help** and follow the troubleshooting procedures.



Test	Description
Ethernet Connection	**Pass:** indicates that the Ethernet interface from your computer is connected to the LAN port of your router. A flashing or solid green LAN LED on the router also signifies that an Ethernet connection is present and that this test is successful. **Fail:** Indicates that the router does not detect the Ethernet interface on your computer.
USB Connection	**Pass:** Indicates that the USB interface from your computer is connected to router properly. **Down:** Indicates that the router does not detect the signal from USB interface.
Wireless Connection	**Pass:** Indicates that the Wireless interface from your computer is connected to the wireless network. **Down:** Indicates that the ADSL router does not detect the wireless network.

ADSL Synchronization	**Pass:** Indicates that the router has detected an ADSL signal from the telephone company. A solid WAN LED on the router also indicates the detection of an ADSL signal from the telephone company. **Fail:** Indicates that the router does not detect a signal from the telephone company's DSL network. The WAN LED will continue to flash green.

If router mode is PPPoE the following screen will be displayed (for your reference).



Chapter 9 Management

The Management section includes the following functions and processes.

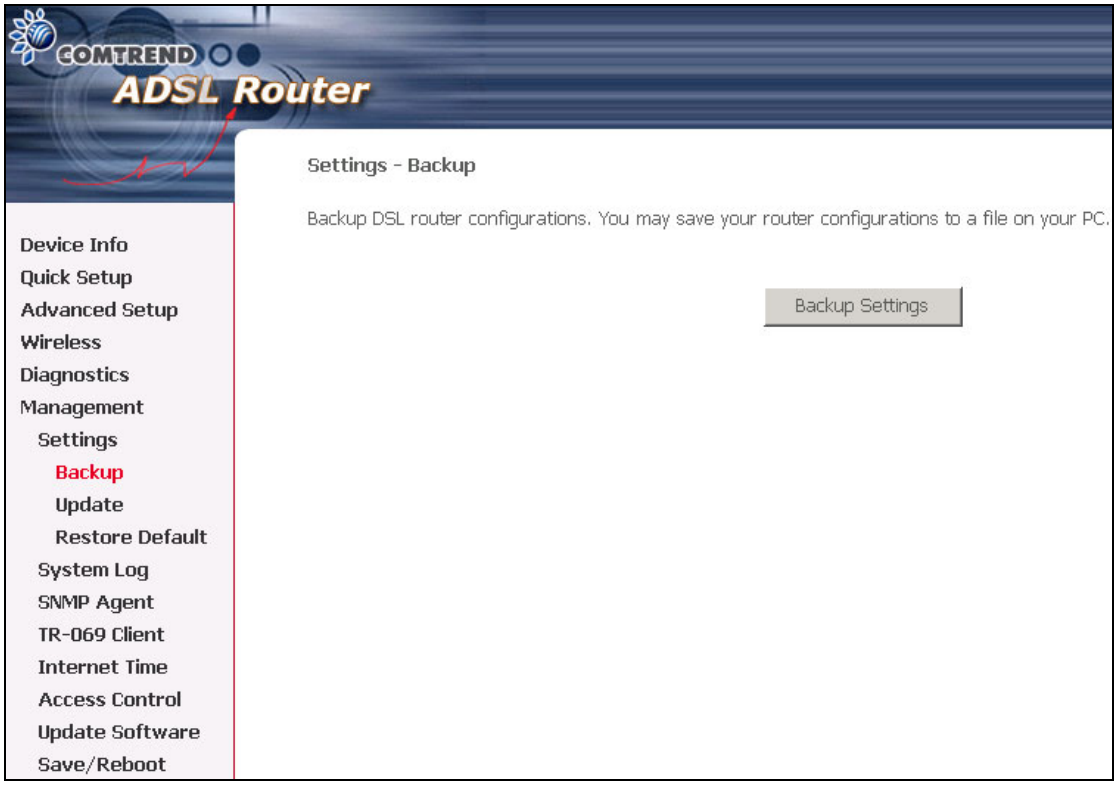
- Settings
- System Log
- SNMP Agent
- TR-069 Client
- Internet Time
- Access Control
- Update Software
- Save/Reboot

9.1 Settings

The Settings option allows you to back up your settings to a file, retrieve the setting file, and restore the settings.

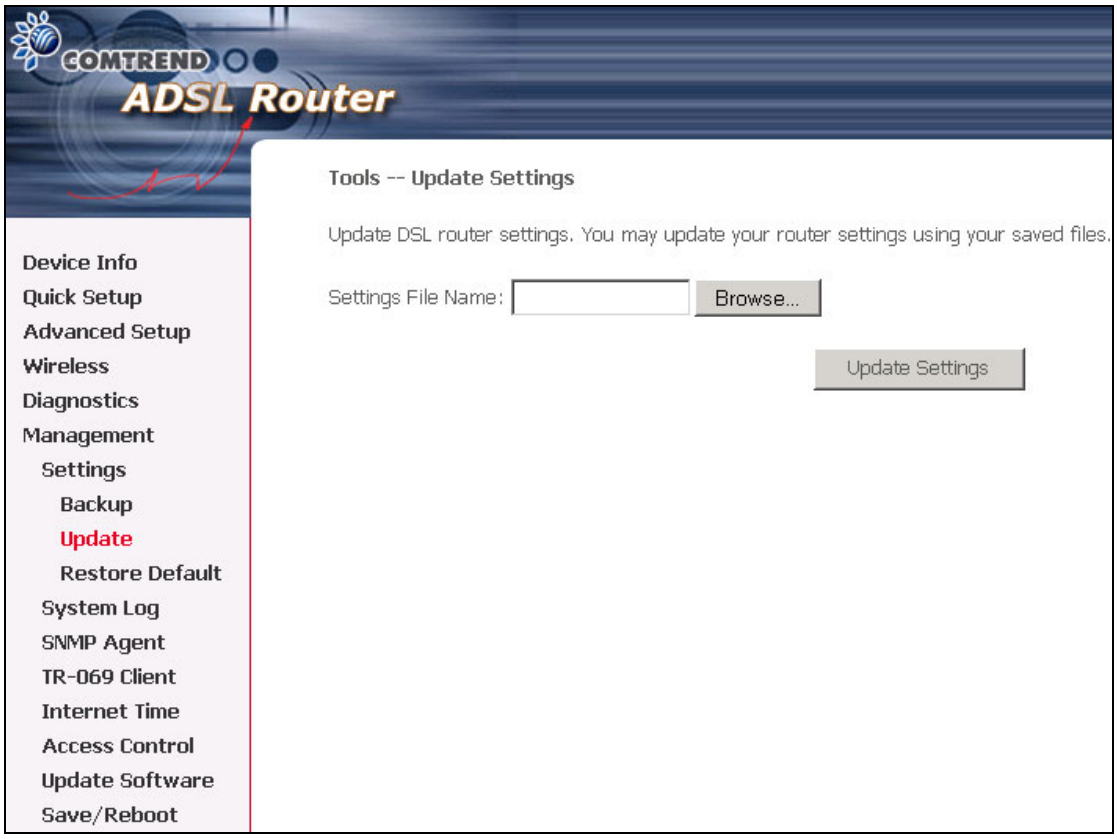
9.1.1 Backup

The Backup option under Management > Settings saves your router configurations to a file on your PC. Click Backup Settings in the main menu. You will be prompted to define the location of the backup file to save. After choosing the file location, click **Backup Settings.** The file will then be saved to the assigned location.



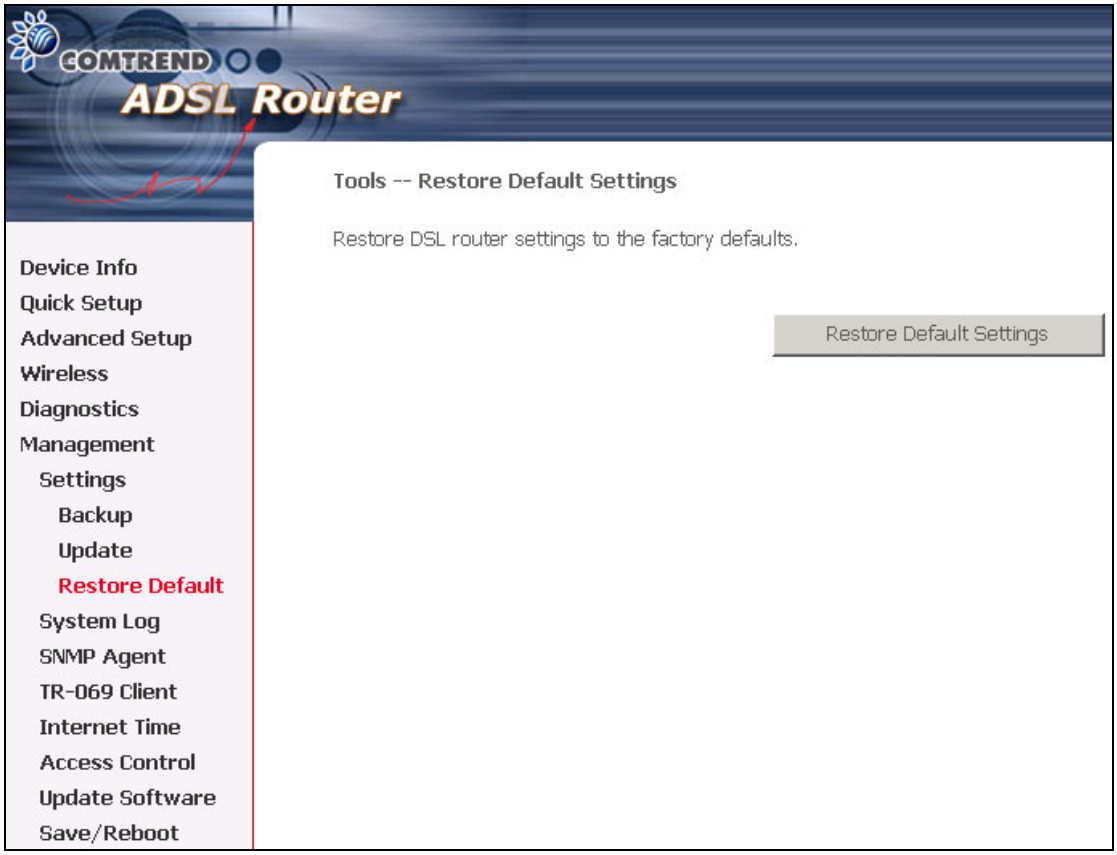
9.1.2 Update

The Update option under Management > Settings updates your router settings using your saved files.



9.1.3 Restore Default

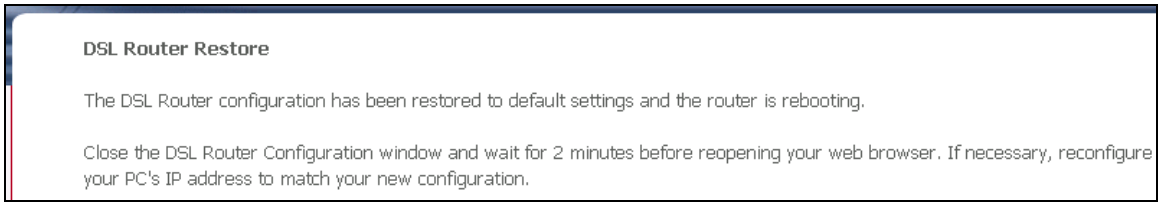
Clicking the Restore Default Configuration option in the Restore Settings screen can restore the original factory installed settings (see section 3.3 Default Settings).



NOTE 1: This entry has the same effect as the hardware reset-to-default button. The device board hardware and the boot loader support the **reset to default** button. If the reset button is continuously pushed for more than 5 seconds, the boot loader will erase the entire configuration data saved on the flash memory.

NOTE 2: Restoring system settings requires a system reboot. This necessitates that the current Web UI session be closed and restarted. Before restarting the connected PC must be configured with a static IP address in the 192.168.1.x subnet in order to configure the router.

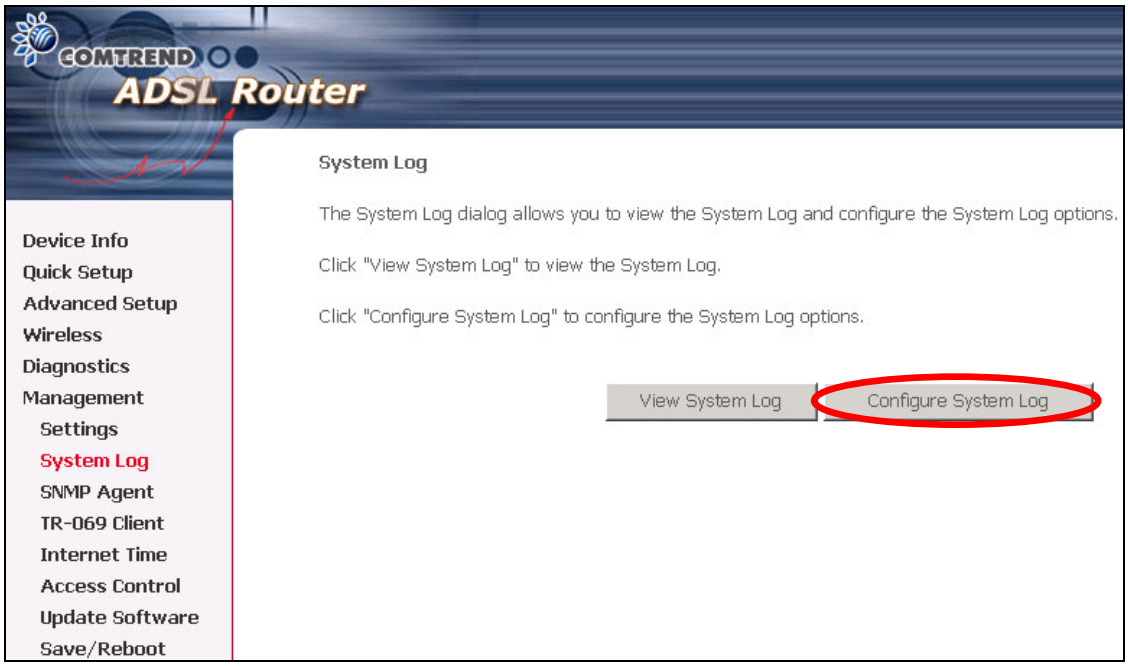
After the Restore Default Configuration button is selected, the following screen appears. Close the window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC IP address to match your new configuration.



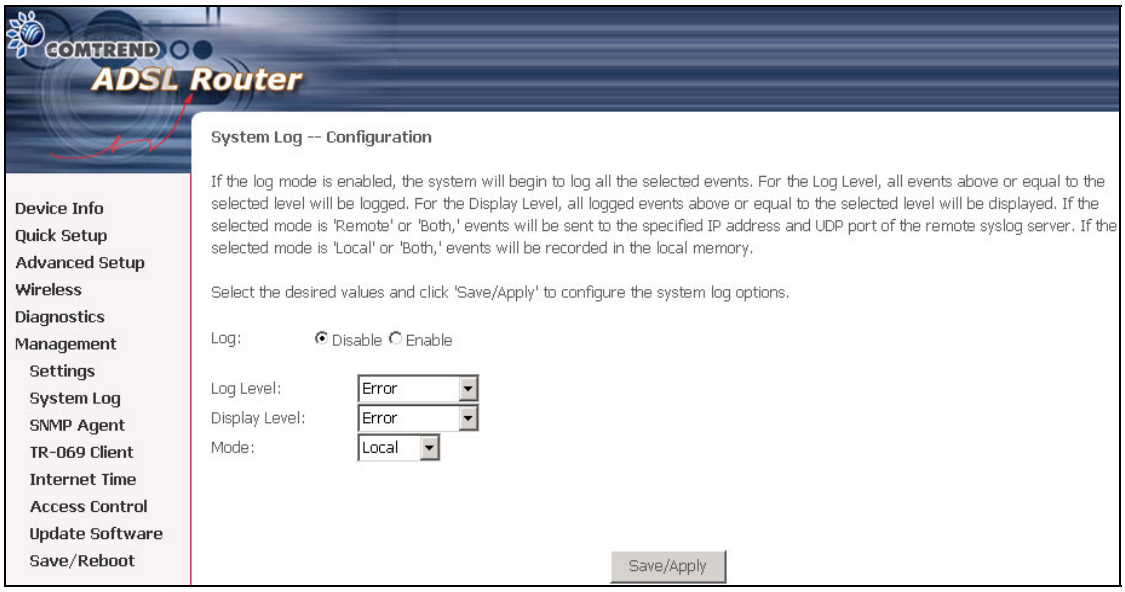
9.2 System Log

The System Log option under Management > Settings allows you to view the system events log, or to configure the System Log options. The default setting of system log is disabled. Follow the steps below to enable and view the system log.

STEP 1: Click **Configure System Log** to display the following screen.



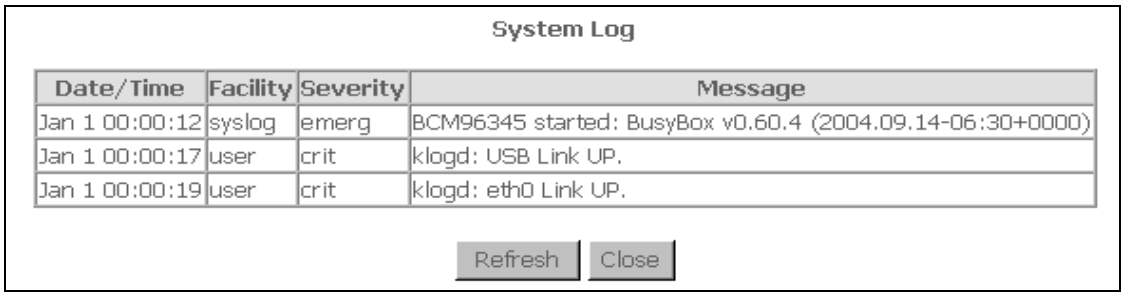
Step 2: Select from the desired Log options described in the following table, and then click **Save/Apply**.



Option	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, tick Enable and then Apply button.
Log level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the device SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging," which is the lowest critical level. The following log levels are • Emergency = system is unusable • Alert = action must be taken immediately • Critical = critical conditions • Error = Error conditions • Warning = normal but significant condition • Notice= normal but insignificant condition • Informational= provides information for reference • Debugging = debug-level messages Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.

Display Level	Allows the user to select the logged events and displays on the **View System Log** page for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote syslog server or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote syslog server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.

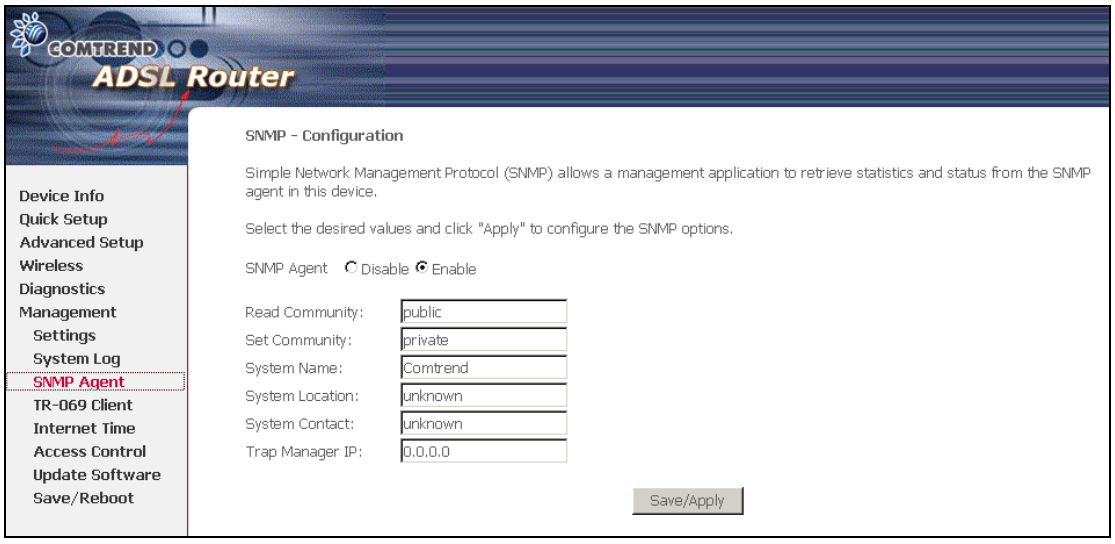
Step 3: Click **View System Log**. The results are displayed as follows.



9.3 SNMP Agent

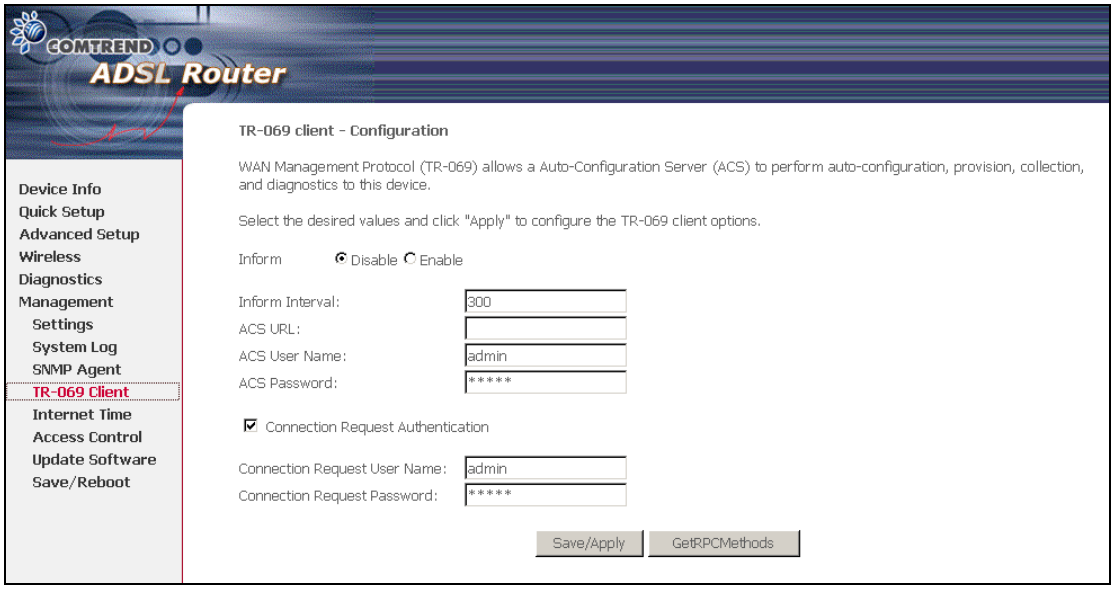
Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this router.

Select or enter the desired values and click **Save/Apply** to configure SNMP options.



9.4 TR-069 Client

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this router.

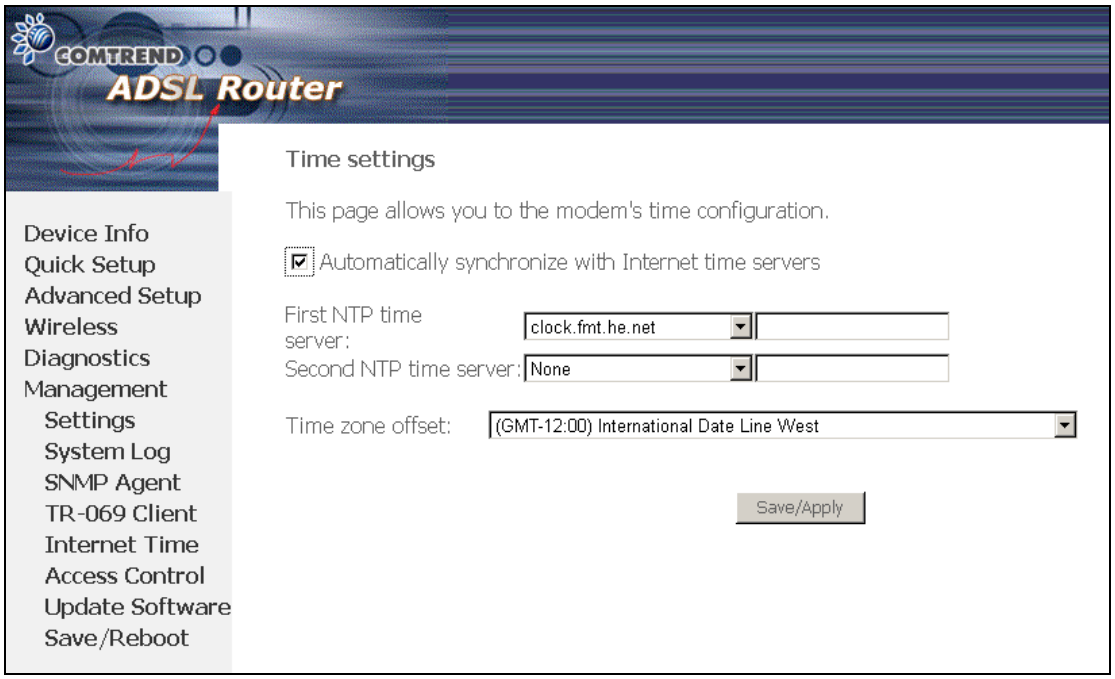


Option	Description
Inform	Disable/Enable TR-069 client on the CPE.
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
ACS User Name	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
ACS Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.
Connection Request Authentication	Enable/Disable authentication of ACS making a Connection Request to the CPE.

Connection Request User Name	Username used to authenticate an ACS making a Connection Request to the CPE.
Connection Request Password	Password used to authenticate an ACS making a Connection Request to the CPE.
Get RPC Methods	This method may be used by a CPE or ACS to discover the set of methods supported by the ACS or CPE it is in communication with. This list may include both standard TR-069 methods (those defined in this specification or a subsequent version) and vendor-specific methods. The receiver of the response MUST ignore any unrecognized methods. Click this button to force the CPE to establish an immediate connection to the ACS.

9.5 Internet Time

The Internet Time option under the Management menu configures the time settings. To automatically synchronize with Internet time servers, tick the corresponding box displayed on the screen; then click **Save/Apply**.



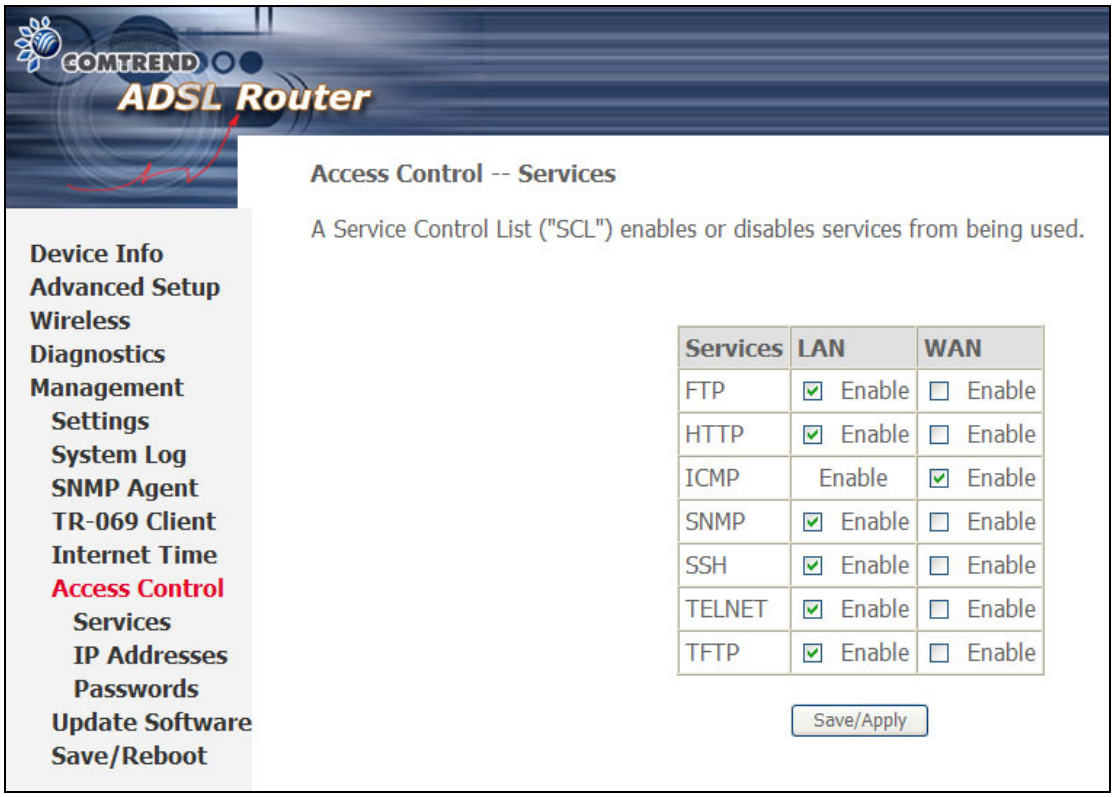
NOTE: This function will not be displayed on the menu when in Bridge mode.

9.6 Access Control

The Access Control option under the Management menu configures three access-related parameters: Services, IP Address and Passwords.

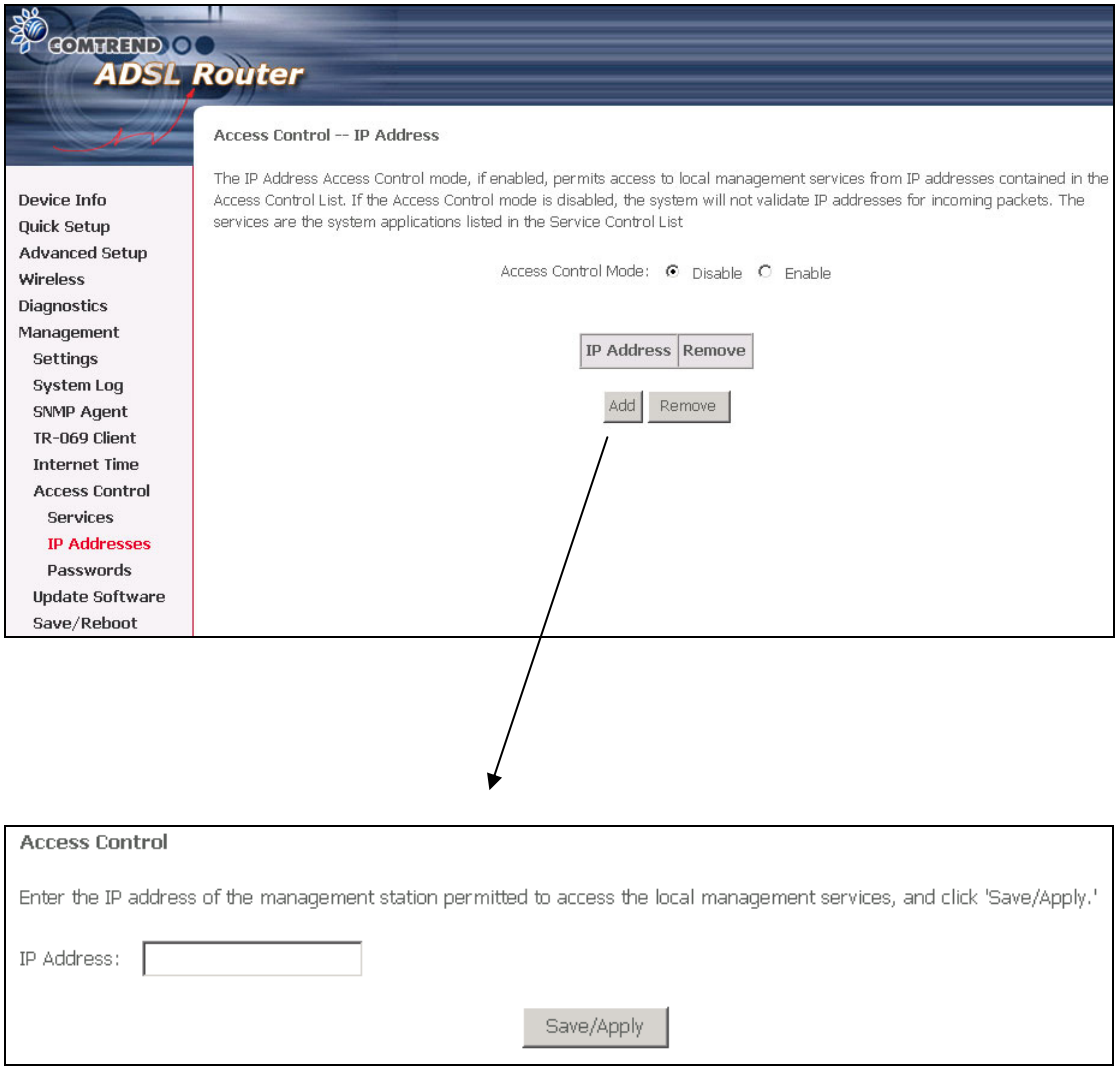
9.6.1 Services

The Services option limits or opens the access services over the LAN or WAN. These services are provided FTP, HTTP, ICMP, SSH (Security Socket Share), TELNET, and TFTP. Enable the service by checking the item in the corresponding checkbox, and then click **Save/Apply**.



9.6.2 Access IP Addresses

The IP Addresses option limits access by IP address. If **Access Control Mode** is enabled, only the IP addresses listed here can access the router. Before enabling it, configure the IP addresses by clicking the **Add** button. Enter the IP address and click **Apply** to allow the PC with this IP address to manage the device.

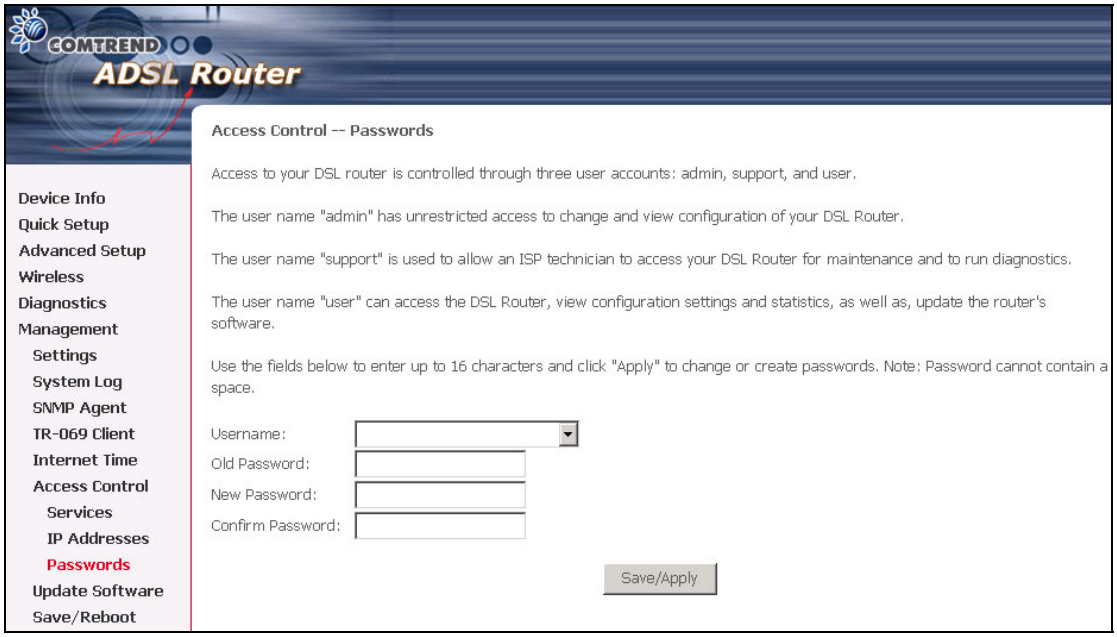


9.6.3 Passwords

The Passwords option configures the access passwords for the router. Access to your router is controlled through three user accounts: root, support, and user.

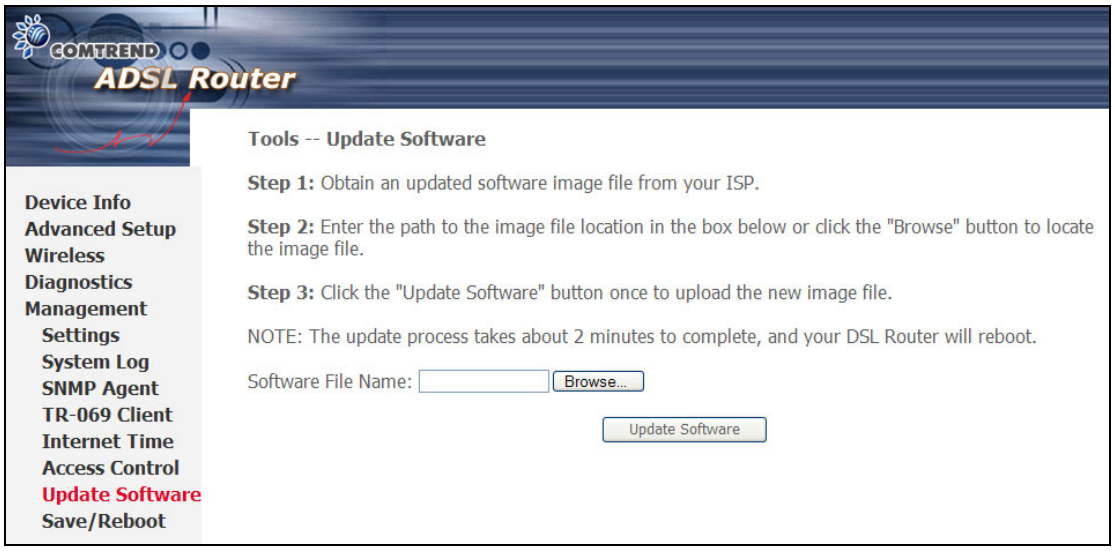
- **root** has unrestricted access to change and view the configuration of your router. It is the top administrative account.
- **support** is intended to allow limited access so that a technical support representative can conduct maintenance and run diagnostics.
- **user** provides the least access control but allows for viewing configuration settings and statistics, as well as, updating software.

Use the fields below to enter up to 16 characters and click Apply to change or create passwords. See section 3.3 Default Settings for default password settings.



9.7 Update Software

The Update Software screen allows you to update the software of the device. Manual software upgrades from a locally stored file can be performed using the following screen. Your ISP will provide this file to you, if necessary.



Step 1: Obtain an updated software image file from your ISP.

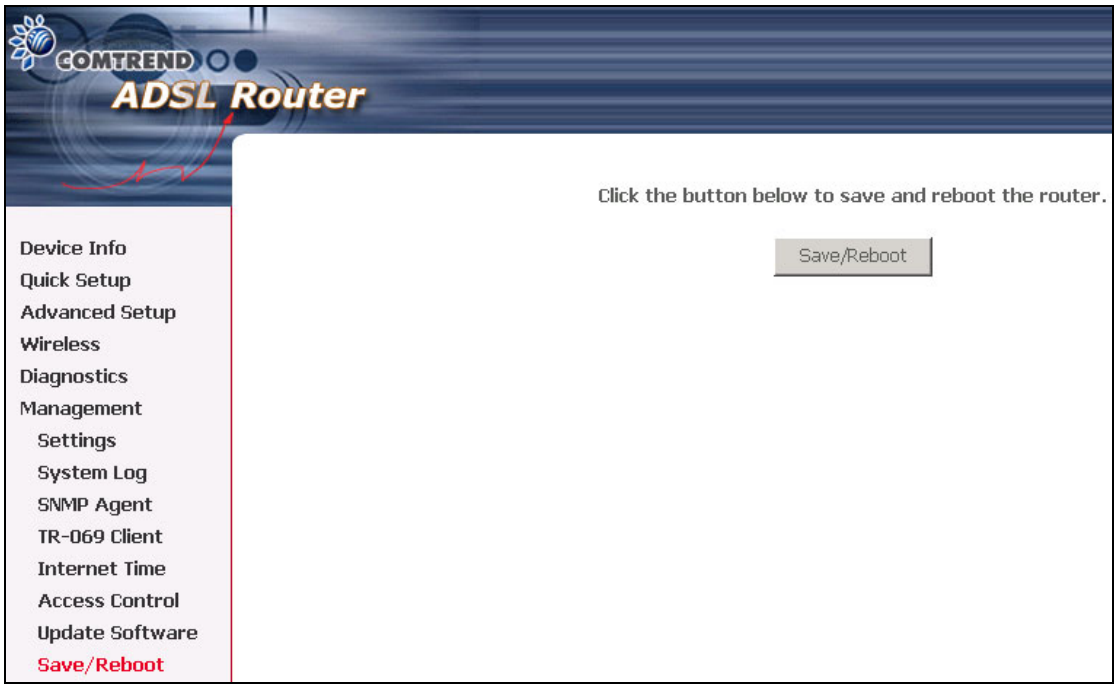
Step 2: Enter the path to the image file location in the box below or click the **Browse** button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

N**OTE:**	The update process takes about 2 minutes to complete, since your router will reboot. Please be patient and restart the browser if necessary.

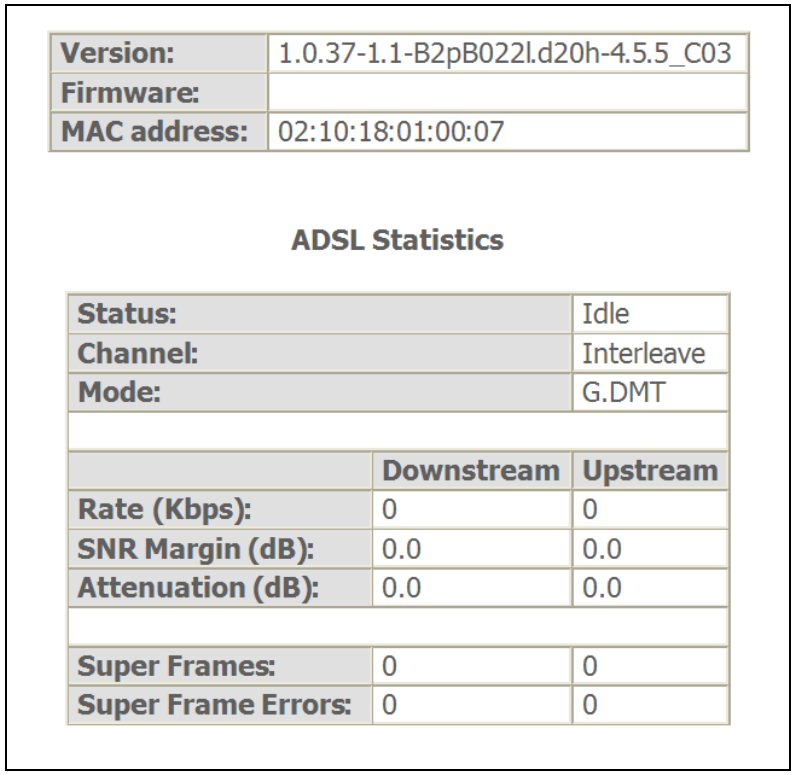
9.8 Save and Reboot

The Save/Reboot button saves the configurations and reboots the router. After clicking it, wait for 2 minutes before attempting to use the user interface. You may need to close and restart the web browser if it does not refresh automatically. You may need to reconfigure your PC IP address to match your new configuration. In this case, see section 3.1 TCP/IP Settings for detailed instructions.



Appendix A: ADSL2 – Slave DSL

Enter this URL http://192.168.1.2 in your browser, to show the screen below.



Version:	1.0.37-1.1-B2pB022l.d20h-4.5.5_C03
Firmware:	
MAC address:	02:10:18:01:00:07

ADSL Statistics

Status:		Idle
Channel:		Interleave
Mode:		G.DMT
	Downstream	**Upstream**
Rate (Kbps):	0	0
SNR Margin (dB):	0.0	0.0
Attenuation (dB):	0.0	0.0
Super Frames:	0	0
Super Frame Errors:	0	0

Version	The version for the second CPU.
Mac Address	The Mac address of the second CPU.
Status	The status of the second CPU.
Channel	Channel type Interleave or Fast for the second CPU. ADSL supports two modes of transport called the fast channel and interleaved channel. The fast channel is meant to transfer latency-critical but error tolerant data streams like real time video. The interleaved path is a slower but reliable path, and can be used for data that is intolerant to errors like file transfer.
Mode	Modulation protocol G.DMT or T1.413 for the second CPU.
Rate (kbps)	Current sync rate for the second CPU.
SNR Margin (dB)	Signal to Noise Ratio (SNR) margin for the second CPU.
Attenuation (dB)	Estimate of average loop attenuation in the downstream direction for the second CPU.
Super Frames	Total number of super frames for the second CPU.
Super Frame Errors	Number of super frames received with errors for the second CPU.

Appendix B: Printer Server

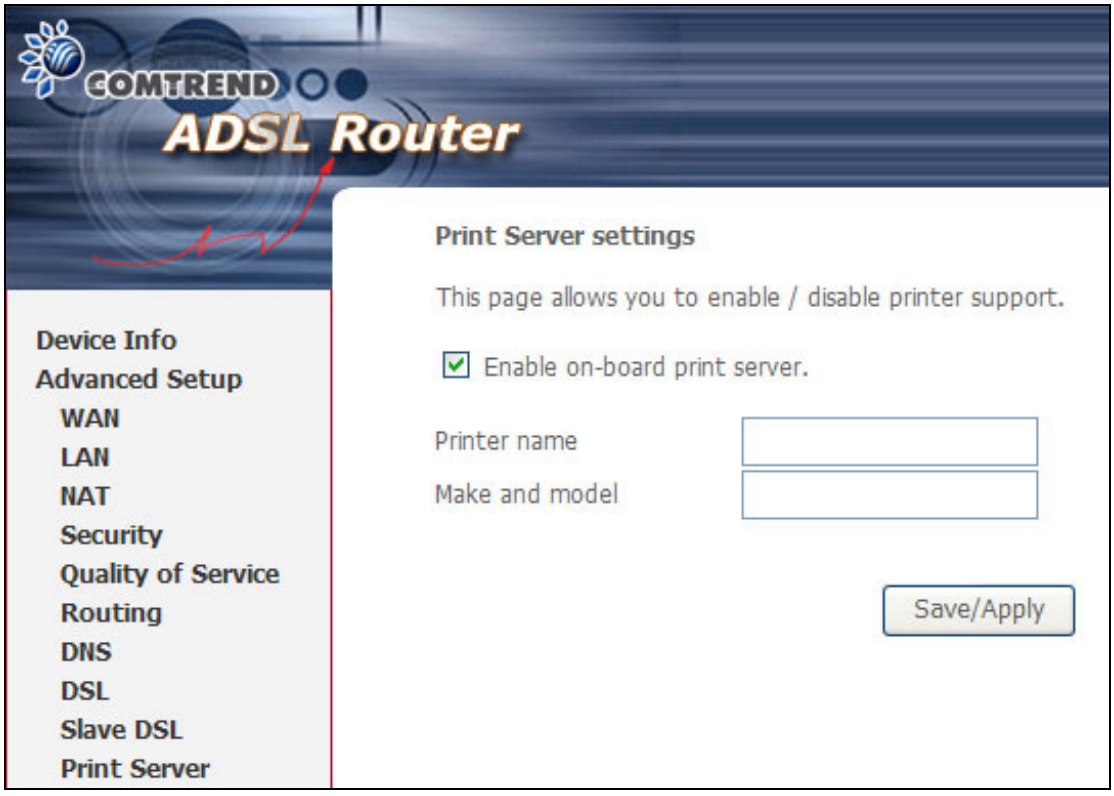
These steps explain the procedure for enabling the Printer Server.

Step 1: Enable Print Server from Web User Interface.

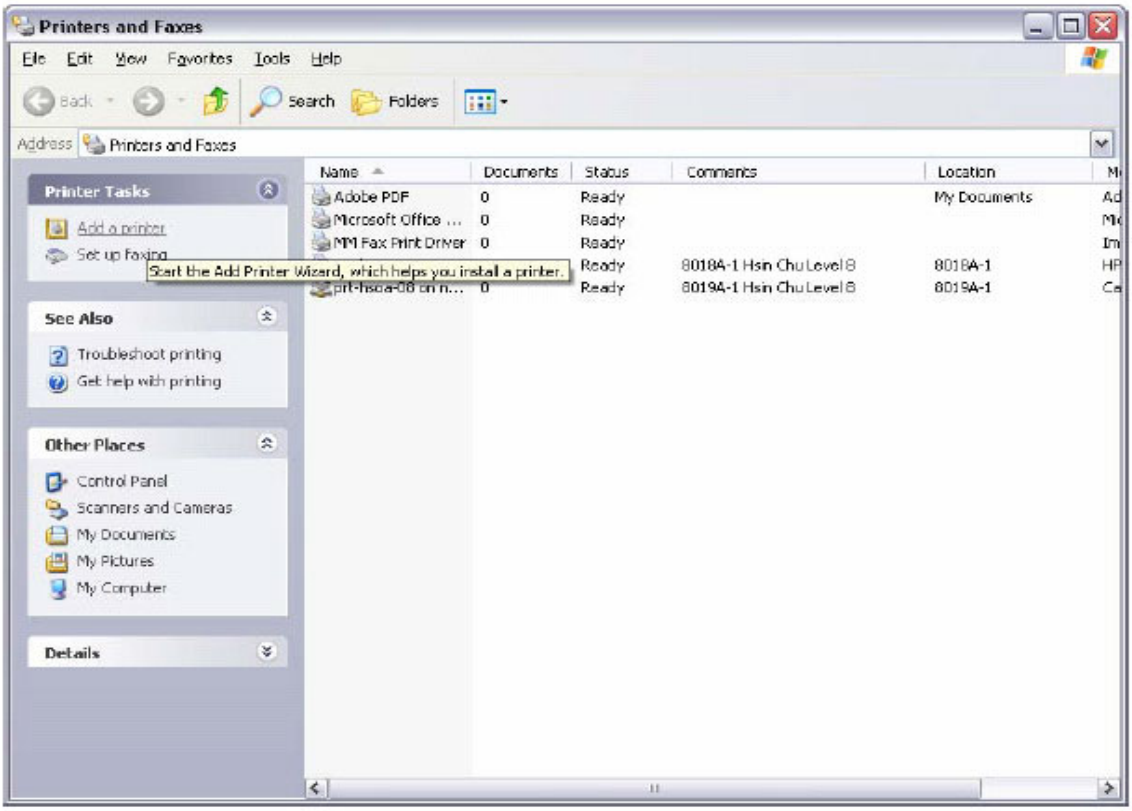
Select **Enable on-board print server** checkbox and

enter **Printer name** and **Make and model**

NOTE:	The **Printer name** can be any text string up to 40 characters. The **Make and model** can be any text string up to 128 characters.



Step 2: Go to the **Printers and Faxes** application in the **Control Panel** and select the **Add a printer** function (as located on the side menu below).



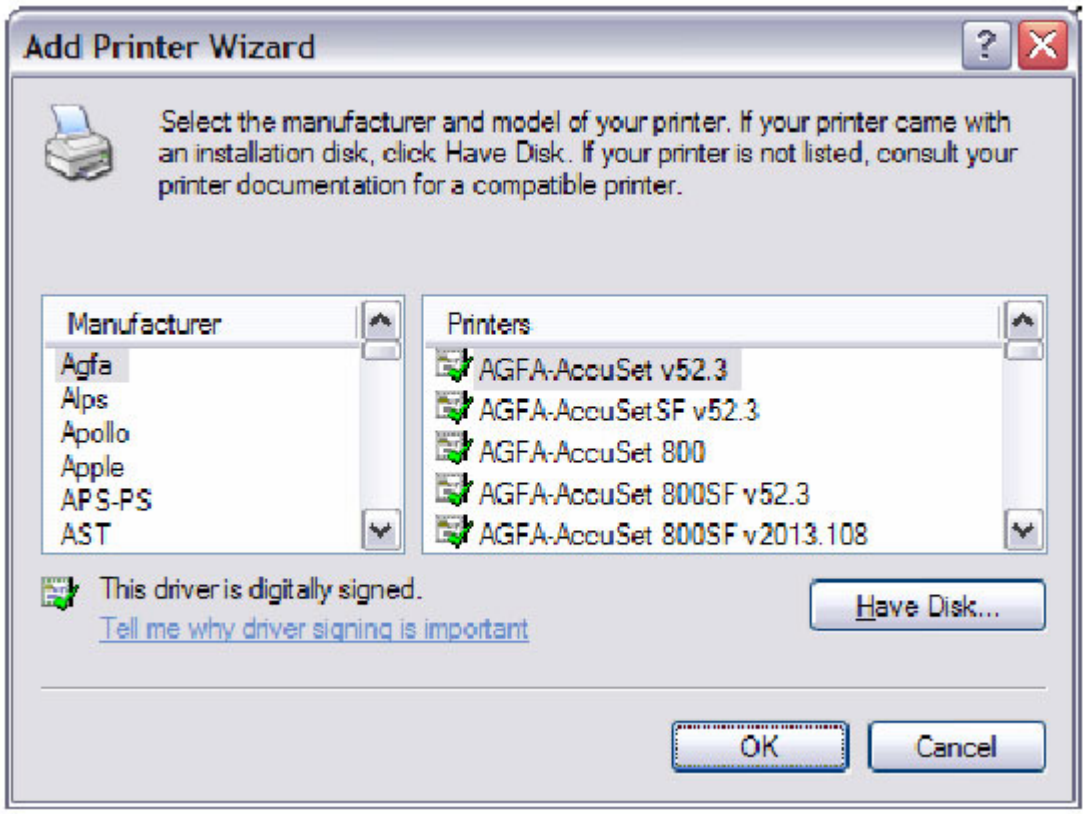
Step 3: Click **Next** to continue, when you see the dialog box below.

Step 4: Select **Network Printer** and click **Next**.

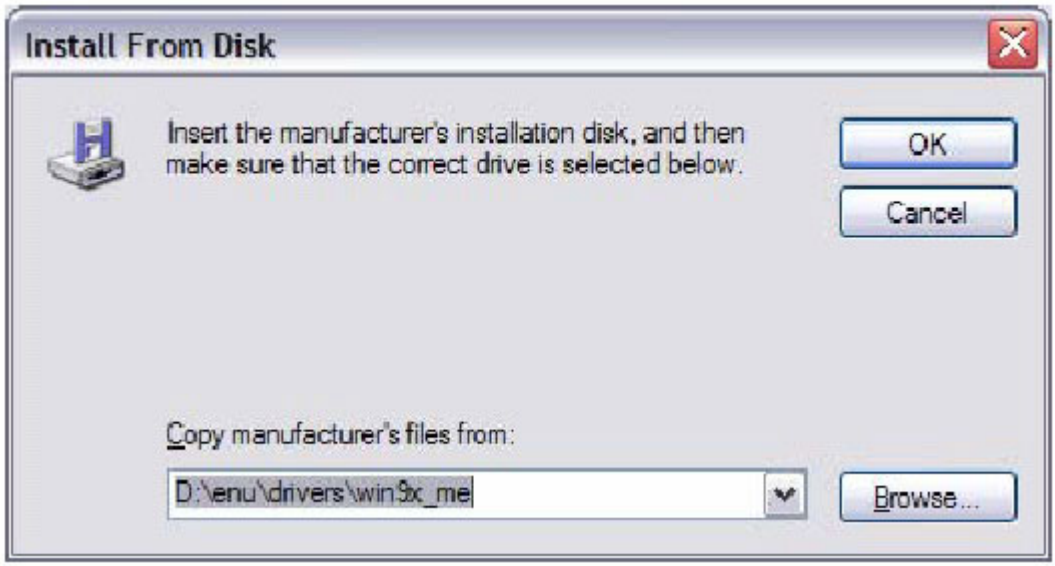
Step 5: Select Connect to a printer on the Internet and enter your printer link. (e.g. http://192.168.1.1:631/printers/hp3845) and click **Next**.

NOTE:	The printer name must be the same name entered in the ADSL modem WEB UI "printer server setting" as in step 1.

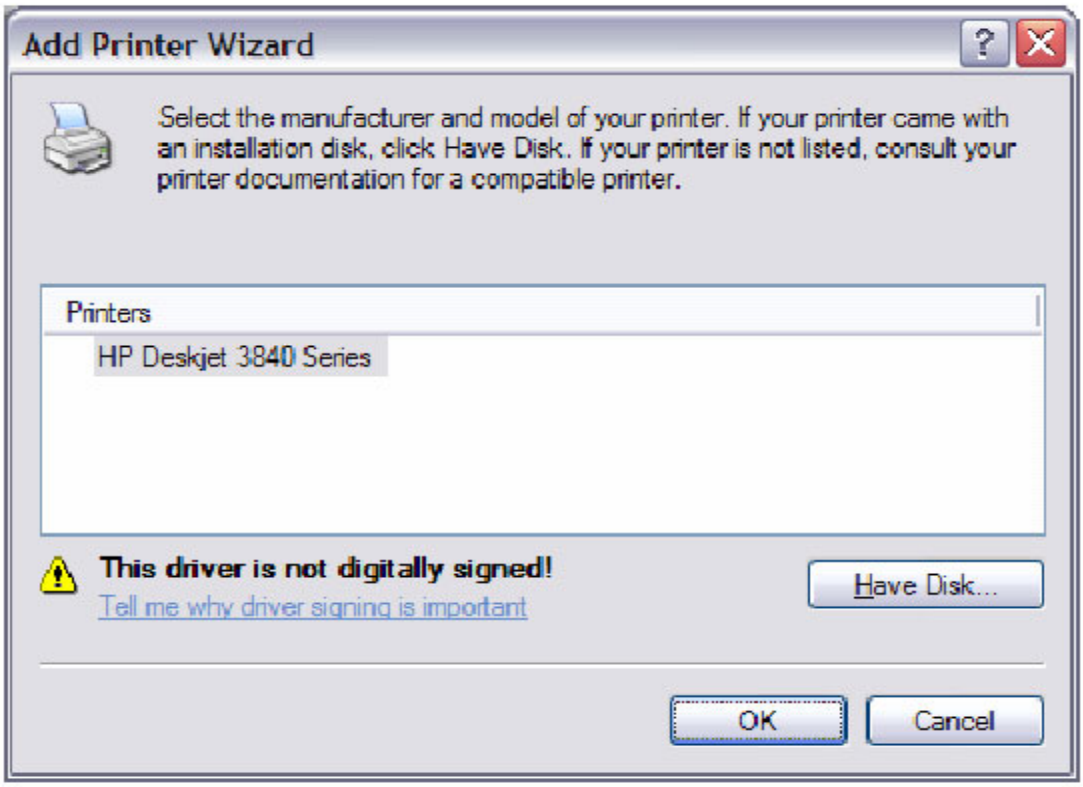
Step 6: Click **Have Disk** and insert the printer driver CD.



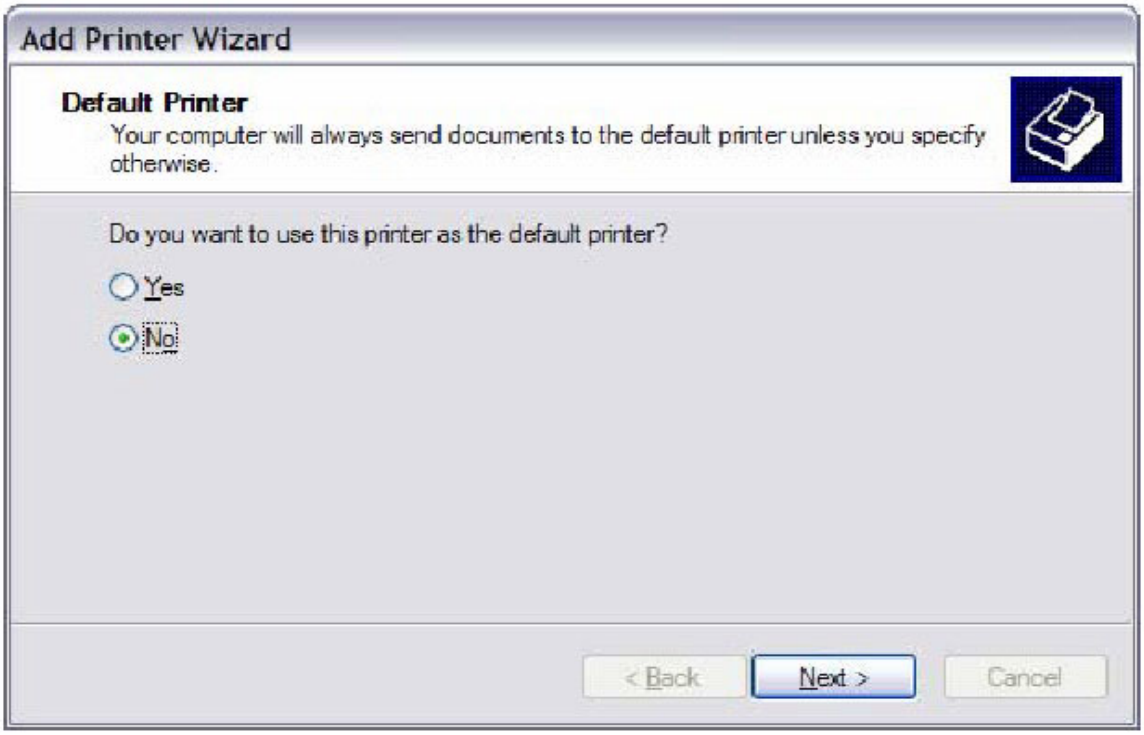
Step 7: Select driver file directory on CD-ROM and click **OK**.



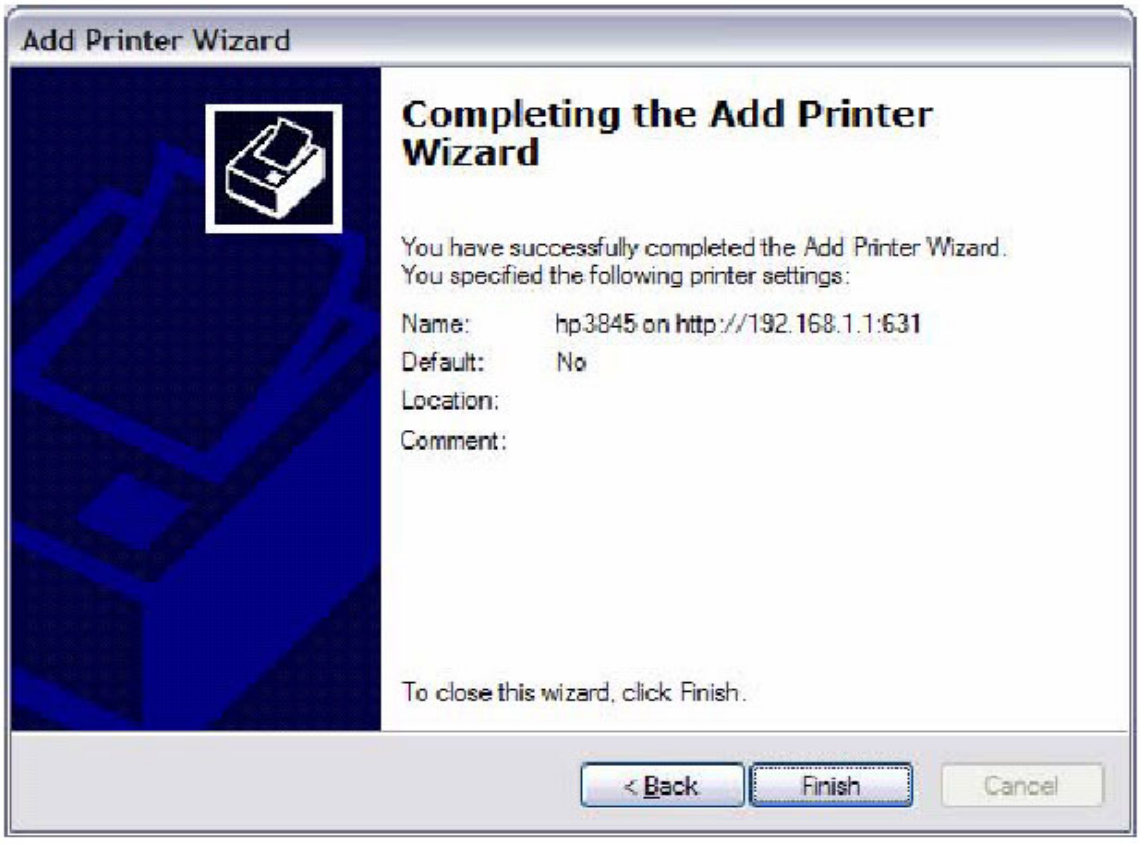
Step 8: Once the printer name appears, click **OK**.



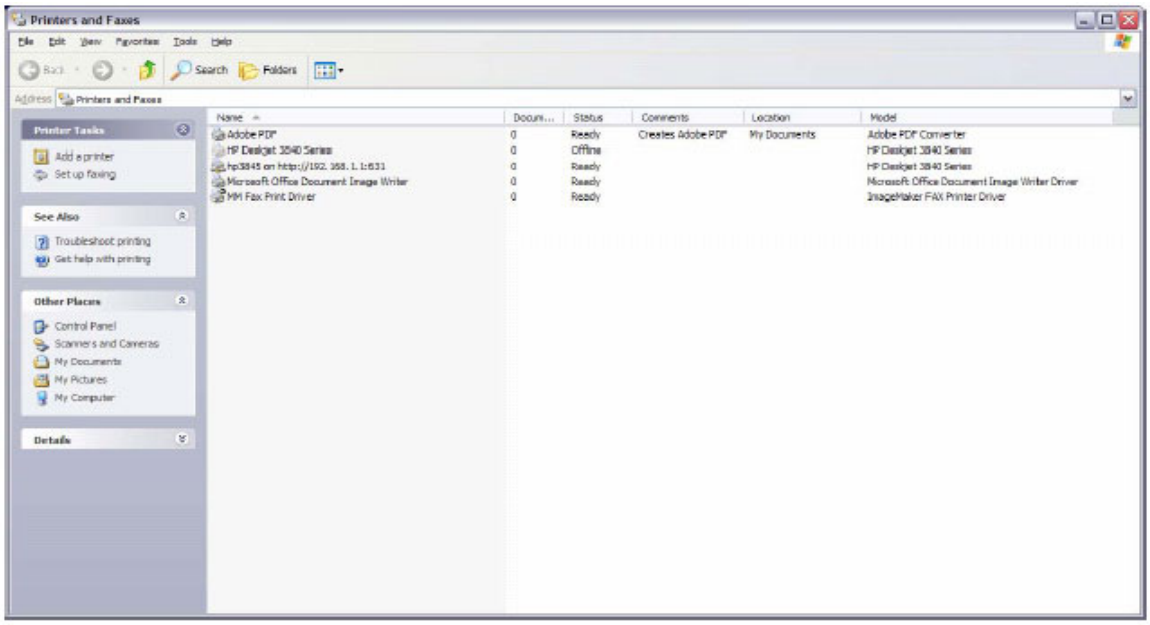
Step 9: Choose **Yes** or **No** for default printer setting and click **Next.**



Step 10: Click "Finish".



Step 11: Check the status of printer from Windows Control Panel, printer window. Status should show as **Ready**.



Appendix C: Firewall

Stateful Packet Inspection

Refers to an architecture, where the firewall keeps track of packets on each connection traversing all its interfaces and makes sure they are valid. This is in contrast to static packet filtering which only examines a packet based on the information in the packet header.

Denial of Service attack

Is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Various DoS attacks the router can withstand are: ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack and Tear Drop.

TCP/IP/Port/Interface filtering rules

These rules help in the filtering of traffic at the Network layer i.e. Layer 3.
When a Routing interface is created "Enable Firewall" must be checked.
Navigate to Advanced Setup -> Security -> IP Filtering, web page.

Outgoing IP Filtering: Helps in setting rules to DROP packets from the LAN interface. By default if Firewall is Enabled all IP traffic from LAN is allowed. By setting up one or more filters, particular packet types coming from the LAN can be dropped.

Filter Name: User defined Filter Name.

Protocol: Can take on any values from: TCP/UDP, TCP, UDP or ICMP

Source IP Address/Source Subnet Mask: Packets with the particular "Source IP Address/Source Subnet Mask" combination will be dropped.
Source Port: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers (portX : portY) will be dropped.

Destination IP Address/Destination Subnet Mask: Packets with the particular "Destination IP Address/Destination Subnet Mask" combination will be dropped.
Destination Port: This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers (portX : portY) will be dropped.

Examples:

1. Filter Name : Out_Filter1
   Protocol : TCP
   Source Address : 192.168.1.45
   Source Subnet Mask : 255.255.255.0
   Source Port : 80
   Dest. Address : NA
   Dest. Sub. Mask : NA
   Dest. Port : NA

This filter will Drop all TCP packets coming from LAN with IP Address/Sub. Mask 192.168.1.45/24 having a source port of 80 irrespective of the destination. All other packets will be Accepted.

2. Filter Name : Out_Filter2
   Protocol : UDP
   Source Address : 192.168.1.45
   Source Subnet Mask : 255.255.255.0
   Source Port : 5060:6060
   Dest. Address : 172.16.13.4
   Dest. Sub. Mask : 255.255.255.0
   Dest. Port : 6060:7070

This filter will drop all UDP packets coming from LAN with IP Address/Sub. Mask 192.168.1.45/24 and a source port in the range of 5060 to 6060, destined to 172.16.13.4/24 and a destination port in the range of 6060 to 7070

Incoming IP Filtering:

Helps in setting rules to ACCEPT packets from the WAN interface. By default all incoming IP traffic from WAN is Blocked, if the Firewall is Enabled. By setting up one or more filters, particular packet types coming from the WAN can be Accepted.

Filter Name: User defined Filter Name.

Protocol: Can take on any values from: TCP/UDP, TCP, UDP or ICMP

Source IP Address/Source Subnet Mask: Packets with the particular "Source IP Address/Source Subnet Mask" combination will be accepted.

Source Port: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers (portX : portY) will be accepted.

Destination IP Address/Destination Subnet Mask: Packets with the particular "Destination IP Address/Destination Subnet Mask" combination will be accepted.

Destination Port: This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers(portX : portY) will be accepted.

The WAN interface on which these rules apply needs to be selected by the user.

Examples:

1. Filter Name : In_Filter1
   Protocol : TCP
   Source Address : 210.168.219.45
   Source Subnet Mask : 255.255.0.0
   Source Port : 80
   Dest. Address : NA
   Dest. Sub. Mask : NA
   Dest. Port : NA

Selected WAN interface: mer_0_35/nas_0_35

This filter will ACCEPT all TCP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Sub. Mask 210.168.219.45/16 having a source port of 80 irrespective of the destination. All other incoming packets on this interface are DROPPED.

2. Filter Name : In_Filter2
   Protocol : UDP
   Source Address : 210.168.219.45
   Source Subnet Mask : 255.255.0.0
   Source Port : 5060:6060
   Dest. Address :192.168.1.45
   Dest. Sub. Mask : 255.255.255.0
   Dest. Port : 6060:7070

This rule will ACCEPT all UDP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Sub. Mask 210.168.219.45/16 and a source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

MAC Layer Filtering:
These rules help in the filtering of traffic at the Layer 2. MAC Filtering is only effective on ATM PVCs configured in Bridge mode. After a Bridge mode PVC is created, navigate to Advanced Setup -> Security -> MAC Filtering web page.

Global Policy:
When set to Forwarded the default filter behavior is to
Forward all MAC layer frames except those explicitly stated in the rules.
Setting it to Blocked changes the default filter behavior to Drop all
MAC layer frames except those explicitly stated in the rules.

To setup a rule:

Protocol Type: Can be PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI or IGMP.

Destination MAC Address: Of the form, XX:XX:XX:XX:XX:XX. Frames with this particular destination address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

Source MAC Address: Of the form, XX:XX:XX:XX:XX:XX. Frames with this particular source address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

Frame Direction:
LAN <=> WAN --> All Frames coming/going to/from LAN or to/from WAN.
WAN => LAN --> All Frames coming from WAN destined to LAN.
LAN => WAN --> All Frames coming from LAN destined to WAN

User needs to select the interface on which this rule is applied.

Examples:
1.
Global Policy: Forwarded
Protocol Type: PPPoE
Dest. MAC Addr: 00:12:34:56:78
Source MAC Addr: NA
Frame Direction: LAN => WAN

WAN Interface Selected: br_0_34/nas_0_34

Addition of this rule drops all PPPoE frames going from LAN-side to WAN-side with a Dest. MAC Addr. of 00:12:34:56:78 irrespective of its Source MAC Addr. on the br_0_34 WAN interface. All other frames on this interface are forwarded.

2.
Global Policy: Blocked
Protocol Type: PPPoE
Dest. MAC Addr: 00:12:34:56:78:90
Source MAC Addr: 00:34:12:78:90:56
Frame Direction: WAN => LAN

WAN Interface Selected: br_0_34/nas_0_34

Addition of this rule forwards all PPPoE frames going from WAN-side to LAN-side with a Dest. MAC Addr. of 00:12:34:56:78 and Source MAC Addr. of 00:34:12:78:90:56 on the br_0_34 WAN interface. All other frames on this interface are dropped.

Daytime Parental Control

This feature restricts access of a selected LAN device to an outside Network through the router, as per chosen days of the week and the chosen times.

User Name: Name of the Filter.

Browser's MAC Address: Displays MAC address of the LAN device on which the browser is running.

Other MAC Address: If restrictions are to be applied to a device other than the one on which the browser is running, the MAC address of that LAN device is entered.

Days of the Week: Days of the week, when the restrictions are applied.

Start Blocking Time: The time when restrictions on the LAN device are put into effect.

End Blocking Time: The time when restrictions on the LAN device are lifted.

Example:

User Name: FilterJohn
Browser's MAC Address: 00:25:46:78:63:21
Days of the Week: Mon, Wed, Fri
Start Blocking Time: 14:00
End Blocking Time: 18:00

When this rule i.e. FilterJohn is entered, a LAN device with MAC Address of 00:25:46:78:63:21 will be restricted access to the outside network on Mondays, Wednesdays and Fridays, from 2pm to 6pm. On all other days and time this device will have access to the outside Network.

Appendix D: Pin Assignments

Line port (RJ14)

Pin	Definition	Pin	Definition
1	-	4	ADSL_TIP1
2	ADSL_TIP2	5	ADSL_RING2
3	ADSL_RING1	6	-

LAN Port (RJ45)

Pin	Definition	Pin	Definition
1	Transmit data+	5	NC
2	Transmit data-	6	Receive data-
3	Receive data+	7	NC
4	NC	8	NC

Appendix E: Specifications

Rear Panel

RJ14 X1 for ADSL2+ bonded, RJ45 X 4 for LAN, Reset Button X 1,
Power switch X 1, optional USB host/device

ADSL

ADSL standard	ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2 AnnexM
ADSL2+ Bonded	Downstream : 48 Mbps Upstream : 2.6 Mbps

Ethernet

Standard	IEEE 802.3, IEEE 802.3u
10/100 BaseT	Auto-sense
MDI/MDX support	Yes

Wireless

Standard	IEEE802.11g, backward compatible with 802.11b
Encryption	64, 128-bit Wired Equivalent Privacy (WEP) Data Encryption
Channels	11 Channels (US, Canada) 13 Channels (Europe) 14 Channels (Japan)
Data Rate	Up to 54Mbps
WPA/WPA2	Yes
IEEE 802.1x	Yes
WMM	Yes
IEEE 802.1x	Yes

ATM Attributes

RFC 2364 (PPPoA), RFC 2684 (RFC 1483) Bridge/Route; RFC 2516 (PPPoE);
RFC 1577 (IPoA)

Support PVCs	16
AAL type	AAL5
ATM service class	UBR/CBR/VBR
ATM UNI support	UNI3.1/4.0
OAM F4/F5	Yes

Management

Telnet, Web-based management, Configuration backup and restoration

Software upgrade via HTTP, TFTP server, or FTP server

Supports TR-069/TR-098/TR-111 for Remote Management

Bridge Functions

Transparent bridging and learning	IEEE 802.1d
VLAN support	Yes
Spanning Tree Algorithm	Yes
IGMP Proxy	Yes

Routing Functions

Static route, RIP, and RIPv2, NAT/PAT, DHCP Server/DHCP Relay, DNS Relay, ARP

Security Functions

Authentication protocols: PAP, CHAP, TCP/IP/Port filtering rules, Port triggering/Forwarding, Packet and MAC address filtering, access control, SSH

Application Passthrough

PPTP, L2TP, IPSec, VoIP, Yahoo messenger, ICQ, RealPlayer, NetMeeting, MSN, X-box, etc

OS Supported for USB driver

Windows 2000/XP/ME/98SE

Power Supply

External power adapter 110 VDC or 220 VDC, 15VDC /1.6A

Environment Condition

Operating temperature 0 ~ 45 degrees Celsius

Relative humidity 5 ~ 95% (non-condensing)

Dimensions: 205 mm (W) x 48 mm (H) x 145 mm (D)

Certifications: FCC Part 15 class B, FCC Part 68, CE

NOTE: Specifications are subject to change without notice

Appendix F: SSH Client

Linux OS comes with ssh client. Microsoft Windows does not have ssh client but there is a public domain one "putty" that you can download.
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

To access the router using Linux ssh client:
From LAN: Use the router WEB UI to enable SSH access from LAN.
(default is enabled)
type: ssh -l admin 192.168.1.1

From WAN: From the router, use WEB UI to enable SSH access from WAN.
type: ssh -l support xx.xx.xx.xx (router WAN IP address)

To access the router using Windows putty ssh client:
From LAN: Use the router WEB UI to enable SSH access from LAN
(default is enabled)
type: putty -ssh -l admin 192.168.1.1

From WAN: From the router, use WEB UI to enable SSH access from WAN.
type: putty -ssh -l support xx.xx.xx.xx (router WAN IP address)